<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco IOS 15.4

Effective date of registration: 11/26/2014</td>
<td>
show aaa method-lists
To display all the named method lists defined in the authentication, authorization, and accounting (AAA) subsystem, use the show aaa method-listscommand in user EXEC or privileged EXEC mode.
show aaa method-lists {accounting| all| authentication| authorization}
Syntax Description
<table>
<tr><td>accounting</td><td>Displays method lists defined for accounting services.</td></tr>
<tr><td>all</td><td>Displays method lists defined for all services.</td></tr>
<tr><td>authentication</td><td>Displays method lists defined for authentication services.</td></tr>
<tr><td>authorization</td><td>Displays method lists defined for authorization services.</td></tr>
</table>

Cisco IOS Security Command Reference: Commands S to Z at 185 (2013)
</td>
<td>
show aaa method-lists
The show aaa method-lists command displays all the named method lists defined in the specified authentication, authorization, and accounting (AAA) service.
Platform all
Command Mode Privileged EXEC
Command Syntax
show aaa method-lists SERVICE_TYPE
Parameters
• SERVICE_TYPE the service type of the method lists that the command displays.
— accounting accounting services.
— authentication authentication services.
— authorization authorization services.
— all accounting, authentication, and authorization services.

Arista User Manual v. 4.14.3F (Rev. 2) at 248 (October 2, 2014)
</td>
</tr>
<tr>
<td>Cisco IOS 15.4

Effective date of registration: 11/26/2014</td>
<td>
<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td>snmp-server community</td><td>Specifies the community access string to define the relationship between the SNMP manager and the SNMP agent to permit access to SNMP.</td></tr>
<tr><td>snmp-server host</td><td>Specifies the recipient (host) of an SNMP notification operation.</td></tr>
</table>

Cisco IOS Security Command Reference: Commands S to Z at 1042 (2013)
</td>
<td>
Configuring the Host
The snmp-server host command specifies the recipient of a SNMP notification. An SNMP host is the recipient of an SNMP trap operation. The snmp-server host command sets the community string if it was not previously configured.

Arista User Manual v. 4.14.3F (Rev. 2) at 1967 (October 2, 2014)
</td>
</tr>
</table>

Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	snmp-server enable traps ipsec
	
	To enable the router to send IP Security (IPSec) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps ipsec**command in global configuration mode. To disable IPSec SNMP notifications, use the **no**form of this command.
	
	snmp-server enable traps ipsec [cryptomap [add| delete| attach| detach]| tunnel [start| stop]| too-many-sas]
	no snmp-server enable traps ipsec [cryptomap [add| delete| attach| detach]| tunnel [start| stop]| too-many-sas]
	
	. . .
	
	SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.
	
	Cisco IOS Security Command Reference: Commands S to Z at 1044 - 1045 (2013)
		snmp-server enable traps
		
		The **snmp-server enable traps** command enables the transmission of Simple Network Management Protocol (SNMP) notifications as traps or inform requests. This command enables both traps and inform requests for the specified notification types. The **snmp-server host** command specifies the notification type (traps or informs). Sending notifications requires at least one **snmp-server host** command.
		
		The **snmp-server enable traps** and **no snmp-server enable traps** commands, without an MIB parameter, specifies the default notification trap generation setting for all MIBs. These commands, when specifying an MIB, controls notification generation for the specified MIB. The **default snmp-server enable traps** command resets notification generation to the default setting for the specified MIB.
		
		Platform all
		Command Mode Global Configuration
		
		Command Syntax
		`snmp-server enable traps [trap_type]`
		`no snmp-server enable traps [trap_type]`
		`default snmp-server enable traps [trap_type]`
		
		Arista User Manual v. 4.14.3F (Rev. 2) at 1990 (October 2, 2014)

Cisco IOS 15.4 Effective date of registration: 11/26/2014	**Command** / **Description** **connect** — Logs in to a host that supports Telnet, rlogin, or LAT. **kerberos clients mandatory** — Causes the **rsh**, **rcp**, **rlogin**, and **telnet** commands to fail if they cannot negotiate the Kerberos Protocol with the remote server. **name connection** — Assigns a logical name to a connection. **rlogin** — Logs in to a UNIX host using rlogin. **show hosts** — Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses. **show tcp** — Displays the status of TCP connections. Cisco IOS Security Command Reference: Commands S to Z at 1192 (2013)	**show hosts** The show hosts command displays the default domain name, name lookup service style, a list of name server hosts, and the static hostname-IP address maps. **Platform** all **Command Mode** EXEC **Command Syntax** `show hosts` Arista User Manual v. 4.14.3F (Rev. 2) at 342 (October 2, 2014)

Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	This command configures the HTTP server to request an X.509v3 certificate from the client in order to authenticate the client during the connection process.
	In the default connection and authentication process, the client requests a certificate from the HTTP server, but the server does not attempt to authenticate the client. Authenticating the client provides more security than server authentication by itself, but not all web clients may be configured for certificate authority (CA) authentication.
	
	Cisco IOS HTTP Services Command Reference at 47 (2011)
		Examples
		• These commands configures the HTTP server to request an X.509 certificate from the client in order to authenticate the client during the connection process.
		`switch(config)#management api http-commands`
		`switch(config-mgmt-api-http-cmds)#protocol https certificate`
		`switch(config-mgmt-api-http-cmds)#`
		
		Arista User Manual v. 4.14.3F (Rev. 2) at 87 (October 2, 2014)

Cisco IOS 15.4 Effective date of registration: 11/26/2014	*start-ip* — Starting IP address that defines the range of addresses in the address pool. *end-ip* — Ending IP address that defines the range of addresses in the address pool. Cisco IOS IP Addressing Services Command Reference at 22 (2011)	*start_addr* The starting IP address that defines the range of addresses in the address pool (IPv4 addresses in dotted decimal notation). *end_addr* The ending IP address that defines the range of addresses in the address pool. (IPv4 addresses in dotted decimal notation). Arista User Manual v. 4.14.3F (Rev. 2) at 1278 (October 2, 2014)
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**clear arp-cache** To refresh dynamically created entries from the Address Resolution Protocol (ARP) cache, use the clear arp-cache command in privileged EXEC mode. **clear arp-cache** [**interface** *type number*	[**vrf** *vrf-name*] *ip-address*] Cisco IOS IP Addressing Services Command Reference at 59 (2011)	**clear arp-cache** The clear arp-cache command refreshes dynamic entries in the Address Resolution Protocol (ARP) cache. Refreshing the ARP cache updates IP address and MAC address mapping information in the ARP table and removes expired ARP entries not yet deleted by an internal, timer-driven process. The command, without arguments, refreshes ARP cache entries for all enabled interfaces. With arguments, the command refreshes cache entries for the specified interface. Executing clear arp-cache for all interfaces can result in extremely high CPU usage while the tables are resolving. Platform all Command Mode Privileged EXEC Command Syntax `clear arp-cache` [*VRF_INSTANCE*] [*INTERFACE_NAME*] Arista User Manual v. 4.14.3F (Rev. 2) at 1255 (October 2, 2014)

Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	ip address
	
	To set a primary or secondary IP address for an interface, use the **ip address** command in interface configuration mode. To remove an IP address or disable IP processing, use the no form of this command.
	
	ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
	no ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
	
	Cisco IOS IP Addressing Services Command Reference at 166 (2011)
	
	An interface can have one primary IP address and multiple secondary IP addresses. Packets generated by the Cisco IOS software always use the primary IP address. Therefore, all routers and access servers on a segment should share the same primary network number.
	
	Hosts can determine subnet masks using the Internet Control Message Protocol (ICMP) mask request message. Routers respond to this request with an ICMP mask reply message.
	
	You can disable IP processing on a particular interface by removing its IP address with the **no ip address** command. If the software detects another host using one of its IP addresses, it will print an error message on the console.
	
	The optional **secondary** keyword allows you to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and Address Resolution Protocol (ARP) requests are handled properly, as are interface routes in the IP routing table.
	
	Cisco IOS IP Addressing Services Command Reference at 167 (2011)
		ip address
		
		The **ip address** command configures the IPv4 address and connected subnet on the configuration mode interface. Each interface can have one primary address and multiple secondary addresses.
		
		The **no ip address** and **default ip address** commands remove the IPv4 address assignment from the configuration mode interface. Entering the command without specifying an address removes the primary and all secondary addresses from the interface. The primary address cannot be deleted until all secondary addresses are removed from the interface.
		
		Removing all IPv4 address assignments from an interface disables IPv4 processing on that port.
		
		Platform all
		Command Mode Interface-Ethernet Configuration
		Interface-Loopback Configuration
		Interface-Management Configuration
		Interface-Port-channel Configuration
		Interface-VLAN Configuration
		
		Command Syntax
		`ip address ipv4_subnet [PRIORITY]`
		`no ip address [ipv4_subnet] [PRIORITY]`
		`default ip address [ipv4_subnet] [PRIORITY]`
		
		Arista User Manual v. 4.14.3F (Rev. 2) at 1262 (October 2, 2014)

Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	ip nat inside destination
	
	To enable the Network Address Translation (NAT) of a globally unique outside host address to multiple inside host addresses, use the **ip nat inside destination** command in global configuration mode. This command is primarily used to implement TCP load balancing by performing destination address rotary translation. To remove the dynamic association to a pool, use the no form of this command.
	
	ip nat **inside destination** list {*access-list-number* | *name*} **pool** *name* [**mapping-id** *map-id*]
	no ip nat **inside destination** list {*access-list-number* | *name*} **pool** *name* [**mapping-id** *map-id*]
	
	Syntax Description
	list *access-list-number* — Standard IP access list number. Packets with destination addresses that pass the access list are translated using global addresses from the named pool
	list *name* — Name of a standard IP access list. Packets with destination addresses that pass the access list are translated using global addresses from the named pool.
	pool *name* — Name of the pool from which global IP addresses are allocated during dynamic translation.
	
	Cisco IOS IP Addressing Services Command Reference at 405 (2011)
		ip nat pool
		
		The ip nat pool command defines a pool of addresses using start address, end address, and either netmask or prefix length. If its starting IP address and ending IP address are the same, there is only one address in the address pool.
		
		During address translation, the NAT server selects an IP address from the address pool to be the translated source address.
		
		The no ip nat pool removes the corresponding ip nat pool command from *running_config*.
		
		Platform FM6000
		Command Mode Global Configuration
		
		Command Syntax
		`ip nat pool pool_name [ADDRESS_SPAN] SUBNET_SIZE`
		`no ip nat pool pool_name`
		`default ip nat pool pool_name`
		
		Parameters
		• *pool_name* name of the pool from which global IP addresses are allocated.
		
		Arista User Manual v. 4.14.3F (Rev. 2) at 1278 (October 2, 2014)

Cisco IOS 15.4 Effective date of registration: 11/26/2014	**ip nat source** To enable Network Address Translation (NAT) on a virtual interface without inside or outside specification, use the **ip nat source** command in global configuration mode. Cisco IOS IP Addressing Services Command Reference (2011), at 439 **pool** *name* — Name of the pool from which global IP addresses are allocated dynamically. **overload** — (Optional) Enables the router to use one global address for many local addresses. When overloading is configured, the TCP or User Datagram Protocol (UDP) port number of each inside host distinguishes between the multiple conversations using the same local IP address. Cisco IOS IP Addressing Services Command Reference (2011), at 440	**ip nat source dynamic** The ip nat source dynamic command enables Network Address Translation (NAT) of a specified source address for packets sent and received on the configuration mode interface. This command installs hardware translation entries for forward and reverse traffic. When the rule specifies a group, the command does not install the reverse path in hardware. The command may include an access control list to filter packets for translation. . . . **overload** Enables the switch to use one global address for many local addresses. When overloading is configured, the TCP or User Datagram Protocol (UDP) port number of each inside host distinguishes between the multiple conversations using the same local IP address. **pool** *pool_name* The name of the pool from which global IP addresses are allocated dynamically. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1279

Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	ip nat pool
	
	To define a pool of IP addresses for Network Address Translation (NAT), use the ip nat poolcommand inglobal configuration mode. To remove one or more addresses from the pool, use the **no** form of this command.
	
	ip nat pool *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*} [**add-route**] [**type** {match-host | rotary}] [**accounting** *list-name*] [**arp-ping**] [nopreservation]
	no ip nat pool *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*} [**add-route**] [**type** {match-host | rotary}] [**accounting** *list-name*] [**arp-ping**] [nopreservation]
	
	Syntax Description
	name — Name of the pool
	start-ip — Starting IP address that defines the range of addresses in the address pool.
	end-ip — Ending IP address that defines the range of addresses in the address pool
	netmask *netmask* — Specifies the network mask that indicates which address bits belong to the network and subnetwork fields and which bits belong to the host field. Specify the netmask of the network to which the pool addresses belong.
	prefix-length *prefix-length* — Specifies the number that indicates how many bits of the netmask are ones (how many bits of the address indicate network). Specify the netmask of the network to which the pool addresses belong.
	
	Cisco IOS IP Addressing Services Command Reference (2011), at 422
	
	This command defines a pool of addresses using start address, end address, and either netmask or prefix length. The pool could define an inside global pool, an outside local pool, or a rotary pool.
	
	Cisco IOS IP Addressing Services Command Reference (2011), at 423
		ip nat pool
		
		The **ip nat pool** command defines a pool of addresses using start address, end address, and either netmask or prefix length. If its starting IP address and ending IP address are the same, there is only one address in the address pool.
		
		During address translation, the NAT server selects an IP address from the address pool to be the translated source address.
		
		The **no ip nat pool** removes the corresponding **ip nat pool** command from *running_config*.
		
		Platform FM6000
		Command Mode Global Configuration
		
		Command Syntax
		`ip nat pool pool_name [ADDRESS_SPAN] SUBNET_SIZE`
		`no ip nat pool pool_name`
		`default ip nat pool pool_name`
		
		Parameters
		• *pool_name* name of the pool from which global IP addresses are allocated.
		• *ADDRESS_SPAN* Options include:
		— *start_addr* The starting IP address that defines the range of addresses in the address pool (IPv4 addresses in dotted decimal notation).
		— *end_addr* The ending IP address that defines the range of addresses in the address pool. (IPv4 addresses in dotted decimal notation).
		• *SUBNET_SIZE* this functions as a sanity check to ensure it is not a network or broadcast network. Options include:
		— **netmask** *ipv4_addr* The network mask that indicates which address bits belong to the network and subnetwork fields and which bits belong to the host field. Specify the netmask of the network to which the pool addresses belong (dotted decimal notation).
		— **prefix-length** *<0 to 32>* The number that indicates how many bits of the netmask are ones (how many bits of the address indicate network). Specify the netmask of the network to which the pool addresses belong.
		
		Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1278

Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	ip nat translation (timeout)
	To change the amount of time after which Network Address Translation (NAT) translations time out, use the **ip nat translation** command inglobal configuration mode. To disable the timeout, use the **no** form of this command.
	ip nat translation {**arp-ping-timeout** | dns-timeout | **finrst-timeout** | **icmp-timeout** | **port-timeout** {tcp *port number* | **udp** *port number*} | **pptp** timeout | **routemap entry timeout** | syn **timeout** | **tcp-timeout** | **timeout** | **udp-timeout**} {*seconds* | **never**}
	
	Cisco IOS IP Addressing Services Command Reference (2011), at 446
	
	seconds — Number of seconds after which the specified port translation times out.
	
	Cisco IOS IP Addressing Services Command Reference (2011), at 447
		Use the **ip nat translation tcp-timeout** or **ip nat translation udp-timeout** commands to change the amount of time after which Network Address Translation (NAT) translations time out.
		
		Example
		• This command globally sets the inactive timeout for TCP to 600 seconds.
		`switch(config)# ip nat translation tcp-timeout 600`
		`switch(config)#`
		• This command globally sets the inactive timeout for UDP to 800 seconds.
		`switch#(config)# ip nat translation udp-timeout 800`
		`switch#(config)#`
		
		Arista User Manual 4.14.3F (Rev. 2) (October 2, 2014), at 1247
		
		period The number of seconds after which the specified port translation times out. Value ranges from *0* to *4294967295*. Default value is 86400 (24 hours).
		
		Arista User Manual 4.14.3F (Rev. 2) (October 2, 2014), at 1284

Cisco IOS 15.4 Effective date of registration: 11/26/2014	**Command** — **Description** **show ip dhcp snooping** — Displays the DHCP snooping configuration. Cisco IOS IP Addressing Services Command Reference (2011), at 311	**show ip dhcp snooping** The show ip dhcp snooping command displays the DHCP snooping configuration. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1302

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**show ip dhcp snooping** To display the DHCP snooping configuration, use the **show ip dhcp snooping**command in privileged EXEC mode. **show ip dhcp snooping** . . . **Command** / **Description** **ip dhcp snooping** — Globally enables DHCP snooping. **ip dhcp snooping binding** — Sets up and generates a DHCP binding configuration to restore bindings across reboots. Cisco IOS IP Addressing Services Command Reference (2011), at 673 **ip dhcp snooping vlan** — Enables DHCP snooping on a VLAN or a group of VLANs. Cisco IOS IP Addressing Services Command Reference (2011), at 674	**show ip dhcp snooping** The show ip dhcp snooping command displays the DHCP snooping configuration. Platform Trident Command Mode EXEC Command Syntax `show ip dhcp snooping` Related Commands • ip dhcp snooping globally enables DHCP snooping. • ip dhcp snooping vlan enables DHCP snooping on specified VLANs • ip dhcp snooping information option enables insertion of option-82 snooping data. • ip helper-address enables the DHCP relay agent on a configuration mode interface. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1302
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**Command** / **Description** **dir** — Displays a list of files on a file system. Cisco IOS IP Application Services Command Reference (2013), at 283	**dir** The dir command displays a list of files on a file system. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 139
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**show ip mroute** — Displays the contents of the IP multicast routing table. Cisco IOS IP Switching Command Reference (2013), at 483	The show ip mroute command displays the contents of the IP multicast routing table. • show ip mroute displays information for all routes in the table. • show ip mroute *gp_addr* displays information for the specified multicast group. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1757

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	*community-string* — Password-like community string sent with the notification operation. **Note** You can set this string using the **snmp-server host** command by itself, but Cisco recommends that you define the string using the **snmp-server community** command prior to using the **snmp-server host** command. **Note** The "at" sign (@) is used for delimiting the context information. Cisco IOS IP Switching Command Reference (2013), at 526	• *comm_str* community string (used as password) sent with the notification operation. Although this string can be set with the **snmp-server host** command, the preferred method is defining it with the **snmp-server community** command prior to using this command. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1995
Cisco IOS 15.4 Effective date of registration: 11/26/2014	SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination than traps. Compared to traps, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once; an inform may be tried several times. The retries increase traffic and contribute to a higher overhead on the network. Cisco IOS IP Switching Command Reference (2013), at 530	37.2.2 SNMP Notifications SNMP notifications are messages, sent by the agent, to inform managers of an event or a network condition. A *trap* is an unsolicited notification. An *inform* (or inform request) is a trap that includes a request for a confirmation that the message is received. Events that a notification can indicate include improper user authentication, restart, and connection losses. Traps are less reliable than informs because the receiver does not send any acknowledgment. However, traps are often preferred because informs consume more switch and network resources. A trap is sent only once and is discarded as soon as it is sent. An inform request remains in memory until a response is received or the request times out. An inform may be retried several times, increasing traffic and contributing to higher network overhead. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1963
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**nssa-only** — (Optional) Limits the default advertisement to this NSSA area by setting the propagate (P) bit in the type-7 LSA to zero. Cisco IOS IP Routing:OSPF Command Reference (2013), at 9	*TYPE* area type. Values include: — <no parameter> area is configured as a not-so-stubby area (NSSA). — nssa-only limits the default advertisement to this NSSA area by setting the propagate (P) bit in the type-7 LSA to zero. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1498

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr><td>Cisco IOS 15.4

Effective date of registration: 11/26/2014</td><td>
area nssa translate
To configure a not-so-stubby area (NSSA) and to configure the OSPF Forwarding Address Suppression in Translated Type-5 LSAs feature, use the area nssa translatecommand in router address family topology or router configuration mode. To remove the NSSA distinction from the area, use the no form of this command.

area nssa translate ommandarea area-id nssa translate type7 [always] [suppress-fa] [default-information-originate [metric ospf-metric] [metric-type ospf-link-state-type] [nssa-only]] [no-ext-capability] [no-redistribution] [no-summary]

no area area-id nssa translate type7 [always] [suppress-fa] [default-information-originate [metric ospf-metric] [metric-type ospf-link-state-type] [nssa-only]] [no-ext-capability] [no-redistribution] [no-summary]

Syntax Description
<table>
<tr><td>area-id</td><td>Identifier for the stub area or NSSA. The identifier can be specified as either a decimal value or an IP address.</td></tr>
<tr><td>translate</td><td>Translates one type of link-state advertisement (LSA) to another type of LSA. This keyword takes effect only on an NSSA Area Border Router (ABR) or an NSSA Autonomous System Boundary Router (ASBR).</td></tr>
<tr><td>type7</td><td>(Required) Translates a Type-7 LSA to a Type-5 LSA. This keyword takes effect only on an NSSA ABR or an NSSA ASBR.</td></tr>
<tr><td>always</td><td>(Optional) Configures an NSSA ABR router as a forced NSSA LSA translator. The NSSA ABR router unconditionally translates Type-7 LSAs to Type-5 LSAs. You can configure the always keyword only in router configuration mode, not in router address family topology configuration mode.</td></tr>
</table>

Cisco IOS IP Routing:OSPF Command Reference (2013), at 11
</td><td>
area nssa translate type7 always (OSPFv3)

The area nssa translate type7 always command translates Type-7 link-state advertisement (LSA) to Type-5 of LSAs.

The no area nssa translate type7 always command removes the NSSA distinction from the area.

Platform all
Command Mode Router-OSPF3 Configuration

Command Syntax
<pre>area area_id nssa translate type7 always
no area_id nssa translate type7 always
default area_id nssa translate type7 always</pre>
Parameters
• area_id area number.
Valid formats: integer <1 to 4294967295> or dotted decimal <0.0.0.1 to 255.255.255.255>
Area 0 (or 0.0.0.0) is not configurable; it is always normal.
Running-config stores value in dotted decimal notation.

Example
• This command configures an NSSA ABR router as a forced NSSA LSA translator. The NSSA ABR router unconditionally translates Type-7 LSAs to Type-5 LSAs.

Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at1501
</td></tr>
<tr><td>Cisco IOS 15.4

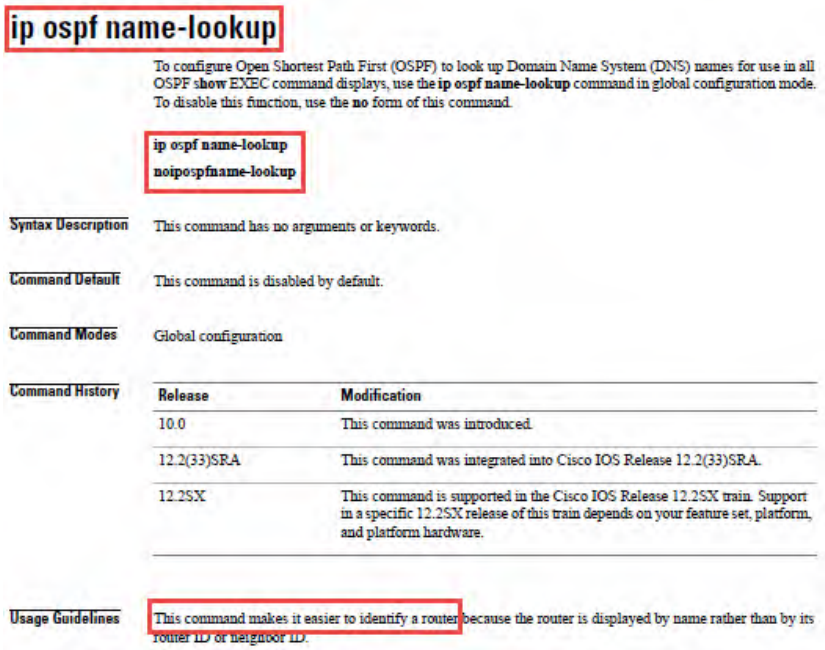
Effective date of registration: 11/26/2014</td><td>
<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td>show ip route</td><td>Displays the current state of the routing table.</td></tr>
</table>

Cisco IOS IP Routing:OSPF Command Reference (2013), at 51
</td><td>
show ip route age

The show ip route age command displays the current state of the routing table and specifies time the route was updated.

Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1313
</td></tr>
</table>

Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	
	ip ospf name-lookup
	To configure Open Shortest Path First (OSPF) to look up Domain Name System (DNS) names for use in all OSPF **show** EXEC command displays, use the **ip ospf name-lookup** command in global configuration mode. To disable this function, use the **no** form of this command.
	ip ospf name-lookup
	noipospfname-lookup
	Syntax Description This command has no arguments or keywords.
	Command Default This command is disabled by default.
	Command Modes Global configuration
	Command History
	Release: 10.0 — Modification: This command was introduced.
	Release: 12.2(33)SRA — Modification: This command was integrated into Cisco IOS Release 12.2(33)SRA.
	Release: 12.2SX — Modification: This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
	Usage Guidelines This command makes it easier to identify a router because the router is displayed by name rather than by its router ID or neighbor ID.
	
	Cisco IOS IP Routing:OSPF Command Reference (2013), at 109
		ip ospf name-lookup
		The ip ospf name-lookup command causes the switch to display DNS names in place of numeric OSPFv2 router IDs in all subsequent OSPFv2 show commands, including:
		• show ip ospf
		• show ip ospf border-routers
		• show ip ospf database <link state list>
		• show ip ospf database database-summary
		• show ip ospf database <link-state details>
		• show ip ospf interface
		• show ip ospf neighbor
		• show ip ospf request-list
		• show ip ospf retransmission-list
		Although this command makes it easier to identify a router the switch relies on a configured DNS server to respond to reverse DNS queries, which may be slower than displaying numeric router IDs.
		The no ip ospf name-lookup and default ip ospf name-lookup commands remove the ip ospf name-lookup command from *running-config*, restoring the default behavior of displaying OSPFv2 router IDs by their numeric value.
		Platform all
		Command Mode Global Configuration
		Command Syntax
		`ip ospf name-lookup`
		`no ip ospf name-lookup`
		`default ip ospf name-lookup`
		
		Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1431

Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	log-adjacency-changes
	
	To configure the router to send a syslog message when an Open Shortest Path First (OSPF) neighbor goes up or down, use the **log-adjacency-changes** command in router configuration mode. To turn off this function, use the **no** form of this command.
	
	log adjacency **changes [detail]**
	no **log-adjacency-changes [detail]**
	
	Syntax Description
	detail — (Optional) Sends a syslog message for each state change, not just when a neighbor goes up or down.
	
	Cisco IOS IP Routing:OSPF Command Reference (2013), at 131
		log-adjacency-changes (OSPFv3)
		
		The **log-adjacency-changes** command configures the switch to send syslog messages when it detects a neighbor has gone up or down. Log message sending is disabled by default. Valid options include:
		• **log-adjacency-changes**: switch sends syslog messages when a neighbor goes up or down (default).
		• **no log-adjacency-changes** disables link state change syslog reporting.
		
		The default option is active when *running-config* does not contain any form of the command. Entering the command in any form replaces the previous command state in *running-config*. The **default log-adjacency-changes** command restores the default state by removing the **log-adjacency-changes** statement from *running-config*.
		
		Platform all
		Command Mode Router-OSPF3 Configuration
		
		Command Syntax
		`log-adjacency-changes [INFO_LEVEL]`
		`no log-adjacency-changes`
		`default log-adjacency-changes`
		
		Parameters
		• *INFO_LEVEL* specifies the type of information displayed. Options include
		— <no parameter> displays all log adjacency change messages
		— **detail** displays syslog message for each state change, not just when a neighbor goes up or down.
		
		Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1518

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**max-metric router-lsa** To configure a router that is running the Open Shortest Path First (OSPF) protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their shortest path first (SPF) calculations, use the **max-metric router-lsa** command in router address family topology or router configuration mode. To disable the advertisement of a maximum metric, use the no form of this command. **max-metric router-lsa** [**external-lsa** [*max-metric-value*]] [**include-stub**] [**on-startup** {*seconds*| **wait-for-bgp**}] [**summary-lsa** [*max-metric-value*]] **no max-metric router-lsa** [**external-lsa** [*max-metric-value*]] [**include-stub**] [**on-startup** {*seconds*| **wait for bgp**}] [**summary** lsa [*max metric value*]] **Syntax Description** **external-lsa** — (Optional) Configures the router to override the external LSA metric with the maximum metric value *max-metric-value* — (Optional) Maximum metric value for LSAs. The configurable range is from 1 to 16777215. The default value is 16711680. include **stub** — (Optional) Configures the router to advertise the maximum metric for stub links in router LSAs. **on-startup** — (Optional) Configures the router to advertise a maximum metric at startup. *seconds* — (Optional) Maximum metric value for the specified time interval. The configurable range is from 5 to 86400 seconds. There is no default timer value for this configuration option. **wait for bgp** — (Optional) Configures the router to advertise a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds. **summary-lsa** — (Optional) Configures the router to override the summary LSA metric with the maximum metric value Cisco IOS IP Routing:OSPF Command Reference (2013), at 136	**max-metric router-lsa (OSPFv3)** The **max-metric router-lsa** command allows the OSPFv3 protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their SPF calculations. The **no max-metric router-lsa** and **default max-metric router-lsa** commands disable the advertisement of a maximum metric. Platform all Command Mode Router-OSPF3 Configuration Command Syntax **max-metric router-lsa** [*EXTERNAL*] [*STUB*] [*STARTUP*] [*SUMMARY*] **no max-metric router-lsa** [*EXTERNAL*] [*STUB*] [*STARTUP*] [*SUMMARY*] **default max-metric router-lsa** [*EXTERNAL*] [*STUB*] [*STARTUP*] [*SUMMARY*] All parameters can be placed in any order. Parameters • *EXTERNAL* advertised metric value. Values include: — <no parameter> Metric is set to the default value of 1. — **external-lsa** Configures the router to override the External LSA / NSSA-External metric with the maximum metric value. — **external-lsa** *<1 to 16777215>* The configurable range is from 1 to 0xFFFFFF. The default value is 0xFF0000. This range can be used with external LSA, summary LSA extensions to indicate the respective metric you want with the LSA. • *STUB* advertised metric type. Values include: — <no parameter> Metric type is set to the default value of 2. — **include-stub** Advertises stub links in router-LSA with the max-metric value (0xFFFF). • *STARTUP* limit scope of LSAs. Values include: — <no parameter> LSA can be translated — **on-startup** Configures the router to advertise a maximum metric at startup (only valid in no and **default** command formats). — **on-startup wait-for-bgp** Configures the router to advertise a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds. — **on-startup** *<5 to 86400>* Sets the maximum metric temporarily after a reboot to originate router-LSAs with the max-metric value. **wait-for-bgp** or an **on-start** time value is not included in **no** and **default** commands. • *SUMMARY* advertised metric value. Values include: — <no parameter> Metric is set to the default value of 1. — **summary-lsa** Configures the router to override the summary LSA metric with the maximum metric value for both type 3 and type 4 Summary LSAs. — **summary-lsa** *<1 to 16777215>* Metric is set to the specified value. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1519

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	The following is sample output from the **showipospf** command when entered without a specific OSPF process ID: Router# **show ip ospf** Routing Process "ospf 201" with ID 10.0.0.1 and Domain ID 10.20.0.1 Supports only single TOS(TOS0) routes Supports opaque LSA SPF schedule delay 5 secs, Hold time between two SPFs 10 secs Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs LSA group pacing timer 100 secs Interface flood pacing timer 55 msecs Retransmission pacing timer 100 msecs Number of external LSA 0. Checksum Sum 0x0 Number of opaque AS LSA 0. Checksum Sum 0x0 Number of DCbitless external and opaque AS LSA 0 Number of DoNotAge external and opaque AS LSA 0 Number of areas in this router is 2. 2 normal 0 stub 0 nssa External flood list length 0 Area BACKBONE(0) Number of interfaces in this area is 2 Area has message digest authentication SPF algorithm executed 4 times Area ranges are Number of LSA 4. Checksum Sum 0x29BEB Number of opaque link LSA 0. Checksum Sum 0x0 Number of DCbitless LSA 3 Number of indication LSA 0 Number of DoNotAge LSA 0 Flood list length 0 Area 172.16.26.0 Number of interfaces in this area is 0 Area has no authentication SPF algorithm executed 1 times Area ranges are 192.168.0.0/16 Passive Advertise Number of LSA 1. Checksum Sum 0x44FD Number of opaque link LSA 0. Checksum Sum 0x0 Number of DCbitless LSA 1 Number of indication LSA 1 Number of DoNotAge LSA 0 Flood list length 0 Cisco IOS IP Routing:OSPF Command Reference (2013), at 174	switch#**show ip ospf** Routing Process "ospf 1" with ID 10.168.103.1 Supports opaque LSA Maximum number of LSA allowed 12000 Threshold for warning message 75% Ignore-time 5 minutes, reset-time 5 minutes Ignore-count allowed 5, current 0 It is an area border router Hold time between two consecutive SPFs 5000 msecs SPF algorithm last executed 00:00:09 ago Minimum LSA interval 5 secs Minimum LSA arrival 1000 msecs Number of external LSA 0. Checksum Sum 0x000000 Number of opaque AS LSA 0. Checksum Sum 0x000000 Number of LSA 27. Number of areas in this router is 3. 3 normal 0 stub 0 nssa Area BACKBONE(0.0.0.0) Number of interfaces in this area is 2 It is a normal area Area has no authentication SPF algorithm executed 153 times Number of LSA 8. Checksum Sum 0x03e13a Number of opaque link LSA 0. Checksum Sum 0x000000 Area 0.0.0.2 Number of interfaces in this area is 1 It is a normal area Area has no authentication SPF algorithm executed 153 times Number of LSA 11. Checksum Sum 0x054e57 Number of opaque link LSA 0. Checksum Sum 0x000000 Area 0.0.0.3 Number of interfaces in this area is 1 It is a normal area Area has no authentication SPF algorithm executed 5 times Number of LSA 6. Checksum Sum 0x02a401 Number of opaque link LSA 0. Checksum Sum 0x000000 Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1391-1392

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**show ip ospf database** To display lists of information related to the Open Shortest Path First (OSPF) database for a specific router, use the **showipospfdatabase** command in EXEC mode. **show** ip ospf [*process id area id*] **database** Cisco IOS IP Routing:OSPF Command Reference (2013), at 184 *link-state-id* — (Optional) Portion of the Internet environment that is being described by the advertisement. The value entered depends on the advertisement's LS type. It must be entered in the form of an IP address. When the link state advertisement is describing a network, the *link-state-id* can take one of two forms: The network's IP address (as in type 3 summary link advertisements and in autonomous system external link advertisements). A derived address obtained from the link state ID. (Note that masking a network links advertisement's link state ID with the network's subnet mask yields the network's IP address.) When the link state advertisement is describing a router, the link state ID is always the described router's OSPF router ID. When an autonomous system external advertisement (LS Type = 5) is describing a default route, its link state ID is set to Default Destination (0.0.0.0). Cisco IOS IP Routing:OSPF Command Reference (2013), at 185	**show ip ospf database <link-state details>** The **show ip ospf database <link-state details>** command displays details of the specified link state advertisements (LSAs). The switch can return link state data about a single area or for all areas on the switch. Platform all Command Mode EXEC Command Syntax **show ip ospf [AREA] database** ***LINKSTATE_TYPE*** *linkstate_id* [***ROUTER***] [***VRF_INSTANCE***] . . . • *linkstate_id* Network segment described by the LSA (dotted decimal notation). Value depends on the LSA type. — When the LSA describes a network, the *linkstate-id* argument is one of the following: The network IP address, as in Type 3 summary link advertisements and in autonomous system external link advertisements. A derived address obtained from the link state ID. Masking a network links the advertisement link state ID with the network subnet mask yielding the network IP address. — When the LSA describes a router, the link state ID is the OSPFv2 router ID of the router. — When an autonomous system external advertisement (Type 5) describes a default route, its link state ID is set to the default destination (0.0.0.0). Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1454

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**show ip ospf interface** To display interface information related to Open Shortest Path First (OSPF), use the show **ip ospf** interface command in user EXEC or privileged EXEC mode. **show ip [ospf] [** *process-id* **] interface [** *type number* **] [brief] [multicast] [topology** [*topology-name*| **base]]** **Syntax Description** *process-id* — (Optional) Process ID number. If this argument is included, only information for the specified routing process is included. The range is 1 to 65535. *type* — (Optional) Interface type. If the *type* argument is included, only information for the specified interface type is included. *number* — (Optional) Interface number. If the *number* argument is included, only information for the specified interface number is included. **brief** — (Optional) Displays brief overview information for OSPF interfaces, states, addresses and masks, and areas on the device. Cisco IOS IP Routing:OSPF Command Reference (2013), at 202	**show ip ospf interface brief** The show ip ospf interface brief command displays a summary of OSPFv2 interfaces, states, addresses and masks, and areas on the router.. Platform all Command Mode EXEC Command Syntax `show ip ospf [PROCESS ID] interface brief [VRF_INSTANCE]` Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1458

Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	shutdown (router OSPF)
	
	To initiate a graceful shutdown of the Open Shortest Path First (OSPF) protocol under the current instance, use the **shutdown** command in router configuration mode. To restart the OSPF protocol, use the **no**form of this command.
	
	shutdown
	no shutdown
	
	Syntax Description This command has no arguments or keywords.
	
	Command Default OSPF stays active under the current instance.
	
	Command Modes Router configuration (config router)
	
	Command History
	Release — **Modification**
	12.2(33)SRC — This command was introduced.
	15.0(1)M — This command was integrated into Cisco IOS Release 15.0(1)M.
	
	Usage Guidelines Use the **shutdown** command in router configuration mode to temporarily shut down a protocol in the least disruptive manner and to notify its neighbors that it is going away. All traffic that has another path through the network will be directed to that alternate path.
	
	Cisco IOS IP Routing:OSPF Command Reference (2013), at 252
		shutdown (OSPFv2)
		
		The shutdown command disables OSPFv2 on the switch. Neighbor routers are notified of the shutdown and all traffic that has another path through the network will be directed to an alternate path.
		
		OSPFv2 is disabled on individual interfaces with the **shutdown (OSPFv2)** command.
		
		The **no shutdown** and **default shutdown** commands enable the OSPFv2 instance by removing the **shutdown** statement from the OSPF block in *running-config*.
		
		Platform all
		Command Mode Router-OSPF Configuration
		
		Command Syntax
		`shutdown`
		`no shutdown`
		`default shutdown`
		
		Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1468

Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	timers lsa arrival
	To set the minimum interval at which the software accepts the same link state advertisement (LSA) from Open Shortest Path First (OSPF) neighbors, use the **timers lsa arrival** command in router configuration mode. To restore the default value, use the **no** form of this command.
	timers lsa arrival *milliseconds*
	no timers lsa arrival
	Syntax Description
	milliseconds — Minimum delay in milliseconds that must pass between acceptance of the same LSA arriving from neighbors. The range is from 0 to 600,000 milliseconds. The default is 1000 milliseconds.
	
	Cisco IOS IP Routing:OSPF Command Reference (2013), at 286
		timers lsa arrival (OSPFv2)
		The **timers lsa arrival** command sets the minimum interval in which the switch accepts the same link-state advertisement (LSA) from OSPF) neighbors.
		The **no timers lsa arrival** and **default timers lsa arrival** commands restore the default maximum OSPFv2 path calculation interval to five seconds by removing the **timers lsa arrival** command from *running-config*.
		Platform all
		Command Mode Router-OSPF Configuration
		Command Syntax
		`timers lsa arrival lsa_time`
		`no timers lsa arrival`
		`default timers lsa arrival`
		Parameters
		• *lsa_time* OSPFv2 minimum interval (seconds). Values range from 1 to 600000 milliseconds. Default is 1000 milliseconds.
		
		Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1469

Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	timers basic (RIP)
	To adjust Routing Information Protocol (RIP) network timers, use the **timers basic** command in router configuration mode. To restore the default timers, use the no form of this command.
	timers basic *update invalid holddown flush*
	no timers basic
	Syntax Description
	update — Rate (in seconds) at which updates are sent. This is the fundamental timing parameter of the routing protocol. The default is 30 seconds.
	invalid — Interval of time (in seconds) after which a route is declared invalid; it should be at least three times the value of the *update* argument. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters into a *holddown* state. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. The default is 180 seconds.
	Cisco IOS IP Routing:RIP Command Reference (2013), at 56
		timers basic (RIP)
		The **timers basic** command configures the update interval, the expiration time, and the deletion time for routes received and sent through RIP. The command requires value declaration of all values.
		• The update time is the interval between unsolicited route responses. The default is 30 seconds.
		• The expiration time is initialized when a route is established and any time an update is received for the route. If the specified period elapses from the last time the route update was received, then the route is marked as inaccessible and advertised as unreachable. However, the route forwards packets until the deletion time expires. The default value is 180 seconds.
		• The deletion time is initialized when the expiration time has elapsed. On initialization of the deletion time, the route is no longer valid; however, it is retained in the routing table for a short time so that neighbors can be notified that the route has been dropped. Upon expiration of the deletion time, the route is removed from the routing table. The default is 120 seconds.
		The **no timers basic** and **default timers basic** commands return the timer values to their default values by removing the **timers-basic** command from *running-config*.
		Platform all
		Command Mode Router-RIP Configuration
		Command Syntax
		`timers basic update_time expire_time deletion_time`
		`no timers basic`
		`default timers basic`
		Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1671

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**distance (IPv6 EIGRP)** To allow the use of two administrative distances--internal and external--that could be a better route to a node, use the **distance**command in router configuration mode. To reset these values to their defaults, use the **no** form of this command. **distance** *internal-distance external-distance* **no distance** **Syntax Description** *internal-distance* — Administrative distance for Enhanced Internal Gateway Routing Protocol (EIGRP) for IPv6 internal routes. Internal routes are those that are learned from another entity within the same autonomous system. The distance can be a value from 1 to 255. *external-distance* — Administrative distance for EIGRP for IPv6 external routes. External routes are those for which the best path is learned from a neighbor external to the autonomous system. The distance can be a value from 1 to 255. Cisco IOS IP Routing: EIGRP Command Reference (2013), at 42	**distance bgp** The **distance bgp** command assigns an administrative distance to routes that the switch learns through BGP. Routers use administrative distances to select a route when two protocols provide routing information to the same destination. Distance values range from 1 to 255; lower distance values correspond to higher reliability. BGP routing tables do not include routes with a distance of 255. The distance command assigns distance values to external, internal, and local BGP routes: • **external:** External routes are routes for which the best path is learned from a neighbor external to the autonomous system. Default distance is 200. • **internal:** Internal routes are routes learned from a BGP entity within the same autonomous system. Default distance is 200. • **local:** Local routes are networks listed with a network router configuration command for that router or for networks that are redistributed from another process. Default distance is 200. The **no distance bgp** and **default distance bgp** commands restore the default administrative distances by removing the **distance bgp** command from *running-config*. **Platform** all **Command Mode** Router-BGP Configuration **Command Syntax** **distance bgp** *external_dist* [***INTERNAL_LOCAL***] **no distance bgp** **default distance bgp** Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1583
Cisco IOS 15.4 Effective date of registration: 11/26/2014	Extended community attributes are used to configure, filter, and identify routes for virtual routing and forwarding instances (VRFs) and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). The **match extcommunity** command is used to configure match clauses that use extended community attributes in route maps. All of the standard rules of match and set clauses apply to the configuration of extended community attributes. Cisco IOS IP Routing: EIGRP Command Reference (2013), at 130	BGP extended communities configure, filter, and identify routes for virtual routing, forwarding instances (VRFs), and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). Extended community clauses provide route target and site of origin parameter options: • **route targets (rt):** This attribute identifies a set of sites and VRFs that may receive routes tagged with the configured route target. Configuring this attribute with a route allows that route to be placed in per-site forwarding tables that route traffic received from corresponding sites. • **site of origin (soo):** This attribute identifies the site from where the Provider Edge (PE) router learns the route. All routes learned from a specific site have the same SOO extended community attribute, whether a site is connected to a single or multiple PE routers. This attribute prevents routing loops resulting from multihomed sites. The SOO attribute is configured on the interface and propagated into a BGP domain by redistribution. The SOO is applied to routes learned from VRFs. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1552

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**shutdown (address-family)** To disable the Enhanced Interior Gateway Routing Protocol (EIGRP) address-family protocol for a specific routing instance without removing any existing address-family configuration parameters, use the **shutdown** command in the appropriate configuration mode. To reenable the EIGRP address-family protocol, use the **no** form of this command. Cisco IOS IP Routing: EIGRP Command Reference (2013), at 276	29.3.4 Disabling IS-IS The IS-IS protocol can be disabled globally on on individuall interfaces. The **shutdown (IS-IS)** command disables the IS-IS protocol for a specific routing instance without removing any existing IS-IS configuration parameters. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1679
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**maximum-paths** — Controls the maximum number of parallel routes an IP routing protocol can support. Cisco IOS IP Routing: BGP Command Reference (November 21, 2012), at 375	**maximum-paths (OSPFv2)** The **maximum-paths** command controls the maximum number of parallel routes that OSPFv2 supports on the switch. The default maximum is 16 paths. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1440
Cisco IOS 15.4 Effective date of registration: 11/26/2014	Together, a route reflector and its clients form a *cluster* . When a single route reflector is deployed in a cluster, the cluster is identified by the router ID of the route reflector. The **bgp cluster-id** command is used to assign a cluster ID to a route reflector when the cluster has one or more route reflectors. Multiple route reflectors are deployed in a cluster to increase redundancy and avoid a single point of failure. When multiple route reflectors are configured in a cluster, the same cluster ID is assigned to all route reflectors. This allows all route reflectors in the cluster to recognize updates from peers in the same cluster and reduces the number of updates that need to be stored in BGP routing tables. Cisco IOS IP Routing: BGP Command Reference (November 21, 2012), at 74	When using route reflectors, an AS is divided into clusters. A cluster consists of one or more route reflectors and a group of clients to which they re-advertise route information. Multiple route reflectors can be configured in the same cluster to increase redundancy and avoid a single point of failure. Each route reflector has a cluster ID. If the cluster has a single route reflector, the cluster ID is its router ID. If a cluster has multiple route reflectors, a 4-byte cluster ID is assigned to all route reflectors in the cluster. All of them must be configured with the same cluster ID so that they can recognize updates from other route reflectors in the same cluster. The **bgp cluster-id** command configures the cluster ID in a cluster with multiple route reflectors. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1549
Cisco IOS 15.4 Effective date of registration: 11/26/2014	The **bgp confederation identifier** command is used to configure a single autonomous system number to identify a group of smaller autonomous systems as a single confederation. A confederation can be used to reduce the internal BGP (iBGP) mesh by dividing a large single autonomous system into multiple subautonomous systems and then grouping them into a single confederation. The subautonomous systems within the confederation exchange routing information like iBGP peers. External peers interact with the confederation as if it were a single autonomous system. Each subautonomous system is fully meshed within itself and has a few connections to other autonomous systems within the confederation. Next hop, Multi Exit Discriminator (MED), and local preference information is preserved throughout the confederation, allowing you to retain a single Interior Gateway Protocol (IGP) for all the autonomous systems. Cisco IOS IP Routing: BGP Command Reference (November 21, 2012), at 77	**BGP Confederations** BGP confederations allow you to break an autonomous system into multiple sub-autonomous systems, and then to group the sub-autonomous systems as a confederation. The sub-autonomous systems exchange routing information as if they are IBGP peers. Specifically, routing updates between sub-autonomous systems include the next-hop, local-preference and MED attributes. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1556

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**bgp redistribute-internal** To configure iBGP redistribution into an interior gateway protocol (IGP), such as IS-IS or OSPF, use the bgp redistribute-internal command in address family or router configuration mode. To stop iBGP redistribution into IGPs, use the no form of this command. bgp redistribute-internal no bgp redistribute-internal Cisco IOS IP Routing: BGP Command Reference (November 21, 2012), at 133	**bgp redistribute-internal (BGP)** The bgp redistribute-internal command enables iBGP redistribution into an interior gateway protocol (IGP), such as IS-IS or OSPF in address family or router BGP configuration mode. The no bgp redistribute-internal and default bgp redistribute-internal commands disable route redistribution from the specified domain by removing the corresponding bgp redistribute-internal command from *running-config*. Platform all Command Mode Router-BGP Configuration Router-BGP Configuration-Address-Family Command Syntax bgp redistribute internal no bgp redistribute internal default bgp redistribute internal Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1576

Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	bgp router-id
	
	To configure a fixed router ID for the local Border Gateway Protocol (BGP) routing process, use the bgp router-id command in router or address family configuration mode. To remove the fixed router ID from the running configuration file and restore the default router ID selection, use the no form of this command.
	
	Router Configuration
	bgp router-id {*ip-address* | **vrf auto-assign**}
	no bgp router-id [**vrf auto assign**]
	
	Address Family Configuration
	bgp router-id {*ip-address*| auto-assign}
	no bgp router-id
	
	Syntax Description
	ip-address — Router identifier in the form of an IP address.
	vrf — Configures a router identifier for a Virtual Routing and Forwarding (VRF) instance.
	auto-assign — Automatically assigns a router identifier for each VRF.
	
	Command Default
	The following behavior determines local router ID selection when this command is not enabled:
	• If a loopback interface is configured, the router ID is set to the IP address of the loopback interface. If multiple loopback interfaces are configured, the router ID is set to the IP address of the loopback interface with the highest IP address.
	• If no loopback interface is configured, the router ID is set to the highest IP address on a physical interface.
	
	Cisco IOS IP Routing: BGP Command Reference (November 21, 2012), at 142
		router-id (BGP)
		
		The **router-id** command configures a fixed router ID for the local Border Gateway Protocol (BGP) routing process.
		
		When the **router-id** command is not configured, the local router ID is set to the following:
		• The loopback IP address when a loopback interface is configured.
		The loopback with the highest IP address is selected when multiple loopback interfaces are configured.
		• The highest IP address on a physical interface when no loopback interfaces are configured.
		
		Important The router-id must be specified if the switch has no IPv4 addresses configured.
		
		The **no router-id** and **default router-id** commands remove the **router-id** command from *running-config*.
		
		Platform all
		Command Mode Router-BGP Configuration
		
		Command Syntax
		`router-id id_num`
		`no router-id [id_num]`
		`default router-id [id_num]`
		
		Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1625

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	The **clear ip bgp** command can be used to initiate a hard reset or soft reconfiguration. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions. Cisco IOS IP Routing: BGP Command Reference (November 21, 2012), at 193	**clear ip bgp** The **clear ip bgp** command removes BGP IPv4 learned routes from the routing table, reads all routes from designated peers, and sends routes to those peers as required. • a hard reset tears down and rebuilds the peering sessions and rebuilds BGP routing tables. • a soft reset uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft resets use stored update information to apply new BGP policy without disrupting the network. Routes that are read or sent are processed through modified route maps or AS-path access lists. The command can also clear the switch's BGP sessions with its peers. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1577

Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	distance bgp
	
	To configure the administrative distance for BGP routes, use the **distance bgp** command in address family or router configuration mode. To return to the administrative distance to the default value, use the no form of this command.
	
	distance bgp *external-distance internal-distance local-distance*
	no distance bgp
	
	Syntax Description
	external distance — Administrative distance for external BGP routes. Routes are external when learned from an external autonomous system. The range of values for this argument are from 1 to 255.
	internal-distance — Administrative distance for internal BGP routes. Routes are internal when learned from peer in the local autonomous system. The range of values for this argument are from 1 to 255.
	local distance — Administrative distance for local BGP routes. Local routes are those networks listed with a network router configuration command, often as back doors, for the router or for the networks that is being redistributed from another process. The range of values for this argument are from 1 to 255.
	
	Cisco IOS IP Routing: BGP Command Reference (November 21, 2012), at 271
		distance bgp
		
		The **distance bgp** command assigns an administrative distance to routes that the switch learns through BGP. Routers use administrative distances to select a route when two protocols provide routing information to the same destination. Distance values range from 1 to 255; lower distance values correspond to higher reliability. BGP routing tables do not include routes with a distance of 255.
		The distance command assigns distance values to external, internal, and local BGP routes:
		• **external**: External routes are routes for which the best path is learned from a neighbor external to the autonomous system. Default distance is 200.
		• **internal**: Internal routes are routes learned from a BGP entity within the same autonomous system. Default distance is 200.
		• **local**: Local routes are networks listed with a network router configuration command for that router or for networks that are redistributed from another process. Default distance is 200.
		The **no distance bgp** and **default distance bgp** commands restore the default administrative distances by removing the **distance bgp** command from *running-config*.
		Platform all
		Command Mode Router-BGP Configuration
		Command Syntax
		`distance bgp external_dist [INTERNAL_LOCAL]`
		`no distance bgp`
		`default distance bgp`
		
		Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1583

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**Expanded Community Lists** Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to configure patterns to match community attributes. The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it will match the earliest part first. For more information about configuring regular expressions, see the "Regular Expressions" appendix of the *Terminal Services Configuration Guide*. Cisco IOS IP Routing: BGP Command Reference (November 21, 2012), at 324	The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it matches the earliest part first. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 107

Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	ip extcommunity-list
	To create an extended community list to configure Virtual Private Network (VPN) route filtering, use the **ip extcommunity-list** command in global configuration mode. To delete the extended community list, use the **no** form of this command.
	To enter IP Extended community-list configuration mode to create or configure an extended community-list, use the **ip extcommunity-list** command in global configuration mode. To delete the entire extended community list, use the **no** form of this command. To delete a single entry, use the **no** form in IP Extended community-list configuration mode.
	Global Configuration Mode CLI
	ip extcommunity-list {*expanded-list* [**permit**| **deny**] [*regular-expression*]| expanded *list-name* [**permit**| **deny**] [*regular expression*]| *standard list* [**permit**| **deny**] [**rt** *value*] [**soo** *value*]| **standard** *list name* [**permit**| **deny**] [**rt** *value*] [**soo** *value*]}
	no ip extcommunity list {*expanded list*| expanded *list name*| *standard list*| **standard** *list name*}
	ip extcommunity list {*expanded list*| expanded *list name*| *standard list*| **standard** *list name*}
	no ip extcommunity-list {*expanded-list*| expanded *list-name*| s*tandard-list*| **standard** *list-name*}
	
	Cisco IOS IP Routing: BGP Command Reference (November 21, 2012), at 326
		ip extcommunity-list standard
		The **ip extcommunity-list standard** command creates an extended community list to configure Virtual Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs).
		• **Route Target (rt)** attribute identifies a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites.
		• **Site of Origin (soo)** attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed.
		The **no ip extcommunity-list standard** and **default ip extcommunity-list standard** commands delete the specified extended community list by removing the corresponding **ip extcommunity-list standard** statement from *running-config*.
		Platform all
		Command Mode Global Configuration
		Command Syntax
		`ip extcommunity-list standard listname FILTER_TYPE COMM_1 [COMM_2...COMM_n]`
		`no ip extcommunity-list standard listname`
		`default ip extcommunity-list standard listname`
		
		Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1591

Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	ip extcommunity-list
	
	To create an extended community list to configure Virtual Private Network (VPN) route filtering, use the **ip extcommunity-list** command in global configuration mode. To delete the extended community list, use the **no** form of this command.
	
	To enter IP Extended community list configuration mode to create or configure an extended community list, use the **ip extcommunity-list** command in global configuration mode. To delete the entire extended community list, use the **no** form of this command. To delete a single entry, use the **no** form in IP Extended community list configuration mode.
	
	Global Configuration Mode CLI
	
	ip extcommunity-list {*expanded-list* [**permit**| **deny**] [*regular-expression*]| **expanded** *list-name* [**permit**| **deny**] [*regular-expression*]| *standard-list* [**permit**| **deny**] [**rt** *value*] [**soo** *value*]| **standard** *list-name* [**permit**| **deny**] [**rt** *value*] [**soo** *value*]}
	
	no ip extcommunity-list {*expanded-list*| **expanded** *list-name*| *standard-list*| **standard** *list-name*}
	
	ip extcommunity-list {*expanded-list*| **expanded** *list-name*| *standard-list*| **standard** *list-name*}
	no ip extcommunity-list {*expanded-list*| **expanded** *list-name*| *standard-list*| **standard** *list-name*}
	
	Cisco IOS IP Routing: BGP Command Reference (November 21, 2012), at 326
		ip extcommunity-list expanded
		
		The ip extcommunity-list expanded command creates an extended community list to configure Virtual Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs). The command uses regular expressions to name the communities specified by the list.
		
		• Route Target (rt) attribute identifies a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites.
		
		• Site of Origin (soo) attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed.
		
		The **no ip extcommunity-list expanded** and **default ip extcommunity-list expanded** commands delete the specified extended community list by removing the corresponding **ip community-list expanded** statement from *running-config*.
		
		Platform all
		Command Mode Global Configuration
		
		Command Syntax
		`ip extcommunity-list expanded listname FILTER_TYPE R_EXP`
		`no ip extcommunity-list expanded listname`
		`default ip extcommunity-list expanded listname`
		
		Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1590

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**Route Target Extended Community Attribute** The route target (RT) extended community attribute is configured with the **rt** keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites. **Site of Origin Extended Community Attribute** The site of origin (SOO) extended community attribute is configured with the **soo** keyword. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same site of origin extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. Cisco IOS IP Routing: BGP Command Reference (November 21, 2012), at 330	**ip extcommunity-list expanded** The **ip extcommunity-list expanded** command creates an extended community list to configure Virtual Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs). The command uses regular expressions to name the communities specified by the list. • **Route Target (rt)** attribute identifies a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites. • **Site of Origin (soo)** attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1590
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**Route Target Extended Community Attribute** The route target (RT) extended community attribute is configured with the **rt** keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites. **Site of Origin Extended Community Attribute** The site of origin (SOO) extended community attribute is configured with the **soo** keyword. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same site of origin extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. Cisco IOS IP Routing: BGP Command Reference (November 21, 2012), at 330	**ip extcommunity-list standard** The **ip extcommunity-list standard** command creates an extended community list to configure Virtual Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs). • **Route Target (rt)** attribute identifies a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites. • **Site of Origin (soo)** attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1591

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**Route Target Extended Community Attribute** The route target (RT) extended community attribute is configured with the **rt** keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites. **Site of Origin Extended Community Attribute** The site of origin (SOO) extended community attribute is configured with the **soo** keyword. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same site of origin extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. Cisco IOS IP Routing: BGP Command Reference (November 21, 2012), at 330	**route targets (rt):** This attribute identifies a set of sites and VRFs that may receive routes tagged with the configured route target. Configuring this attribute with a route allows that route to be placed in per-site forwarding tables that route traffic received from corresponding sites. **site of origin (soo):** This attribute identifies the site from where the Provider Edge (PE) router learns the route. All routes learned from a specific site have the same SOO extended community attribute, whether a site is connected to a single or multiple PE routers. This attribute prevents routing loops resulting from multihomed sites. The SOO attribute is configured on the interface and propagated into a BGP domain by redistribution. The SOO is applied to routes learned from VRFs. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1552
Cisco IOS 15.4 Effective date of registration: 11/26/2014	Extended community attributes are used to configure, filter, and identify routes for virtual routing and forwarding instances (VRFs) and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). Cisco IOS IP Routing: BGP Command Reference (November 21, 2012), at 359	BGP extended communities configure, filter, and identify routes for virtual routing, forwarding instances (VRFs), and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1552

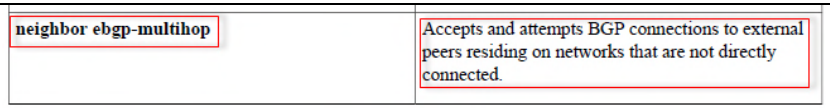
Copyright Registration Information	Cisco	Arista

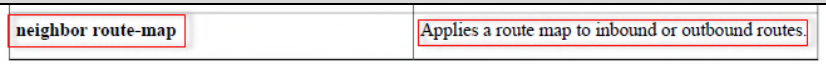
Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	neighbor ebgp-multihop
	
	To accept and attempt BGP connections to external peers residing on networks that are not directly connected, use the **neighbor ebgp-multihop** command in router configuration mode. To return to the default, use the **no** form of this command.
	
	neighbor {*ip-address*| *ipv6-address*| *peer-group-name*} **ebgp-multihop** [*ttl*]
	no neighbor {*ip-address*| *ipv6-address*| *peer-group-name*} **ebgp-multihop**
	
	Cisco IOS IP Routing: BGP Command Reference (November 21, 2012), at 423
		neighbor ebgp-multihop
		
		The **neighbor ebgp-multihop** command programs the switch to accept and attempt BGP connections to the external peers residing on networks not directly connected to the switch. The command does not establish the multihop if the only route to the peer is the default route (0.0.0.0).
		
		The **no neighbor ebgp-multihop** command applies the system default configuration.
		
		The **default neighbor ebgp-multihop** command applies the system default configuration for individual neighbors, and applies the peer group's setting for neighbors that are members of a peer group.
		
		The no neighbor command removes all configuration commands for the neighbor at the specified address.
		
		Platform all
		Command Mode Router-BGP Configuration
		
		Command Syntax
		`neighbor NEIGHBOR_ID ebgp-multihop [hop_number]`
		`no neighbor NEIGHBOR_ID ebgp-multihop`
		`default neighbor NEIGHBOR_ID ebgp-multihop`
		
		Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1597

Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	neighbor local-as
	
	To customize the AS_PATH attribute for routes received from an external Border Gateway Protocol (eBGP) neighbor, or to configure the BGP—Support for iBGP Local-AS feature, use the **neighbor local-as** command in address family or router configuration mode. To disable AS_PATH attribute customization or iBGP Local-AS support, use the **no** form of this command.
	
	neighbor {*ip-address*| *ipv6-address*| *peer-group-name*} **local-as** [*autonomous-system-number* [**no-prepend** [**replace-as** [**dual-as**]]]]
	no neighbor {*ip-address*| *ipv6-address*| *peer-group-name*} **local-as**
	
	. . .
	
	| **no-prepend** | (Optional) Does not prepend the local autonomous system number to any routes received from the eBGP neighbor. |
	
	Cisco IOS IP Routing: BGP Command Reference (November 21, 2012), at 442
		neighbor local-as
		
		The **neighbor local-as** command enables the modification of the AS_PATH attribute for routes received from an eBGP neighbor, allowing the switch to appear as a member of a different autonomous system (AS) to external peers. This switch does not prepend the local AS number to routes received from the eBGP neighbor. The AS number from the local BGP routing process is not prepended.
		
		The **no neighbor local-as** command disables AS_PATH modification for the specified peer or peer group.
		
		The **default neighbor local-as** command disables AS_PATH modification for invidual neighbors, and applies the peer group's setting for neighbors that are members of a peer group.
		
		Platform all
		Command Mode Router-BGP Configuration
		
		Command Syntax
		`neighbor NEIGHBOR_ID local-as as_id no-prepend replace-as`
		`no neighbor NEIGHBOR_ID local-as`
		`default neighbor NEIGHBOR_ID local-as`
		
		Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1601

Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	neighbor remove-private-as
	
	To remove private autonomous system numbers from the autonomous system path (a list of autonomous systems that a route passes through to reach a BGP peer) in eBGP outbound routing updates, use the **neighbor remove private as** command in router configuration, address family configuration, or peer group template mode. To disable this function, use the **no** form of this command.
	
	neighbor {*ip-address*|*peer-group-name*} **remove-private-as** [**all** [**replace-as**]]
	no neighbor {*ip address*|*peer group name*} **remove private as**
	
	Syntax Description
	
	ip address — IP address of the BGP speaking neighbor.
	peer group name — Name of a BGP peer group.
	all — (Optional) Removes all private AS numbers from the AS path in outgoing updates.
	replace-as — (Optional) As long as the **all** keyword is specified, the **replace-as** keyword causes all private AS numbers in the AS path to be replaced with the router's local AS number.
	
	Cisco IOS IP Routing: BGP Command Reference (November 21, 2012), at 479
		neighbor remove-private-as
		
		The **neighbor remove-private-as** command removes private autonomous system numbers from outbound routing updates for external BGP (eBGP) neighbors. When the autonomous system path includes both private and public autonomous system numbers, the *REMOVAL* parameter specifies how the private autonomous system number is removed.
		
		The **no neighbor remove-private-as** command applies the system default (preserves private AS numbers) for the specified peer.
		
		The **default neighbor remove-private-as** command applies the system default for individual neighbors, and applies the peer group's setting for neighbors that are members of a peer group.
		
		The no neighbor command removes all configuration commands for the neighbor at the specified address.
		
		Platform all
		Command Mode Router-BGP Configuration
		
		Command Syntax
		`neighbor NEIGHBOR_ID remove-private-as [REMOVAL]`
		`no neighbor NEIGHBOR_ID remove-private-as`
		`default neighbor NEIGHBOR_ID remove-private-as`
		
		Parameters
		• *NEIGHBOR_ID* IP address or peer group name. Values include:
		— *ipv4_addr* neighbor's IPv4 address.
		— *ipv6_addr* neighbor's IPv6 address.
		— *group_name* peer group name.
		• *REMOVAL* Specifies removal of private autonomous AS number when path includes both private and public numbers. Values include:
		— <no parameter> private AS numbers are not removed.
		— *all* removes all private AS numbers from AS path in outbound updates.
		— *all replace-as* all private AS numbers in AS path are replaced with router's local AS number.
		
		Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1612

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**neighbor route-reflector-client** To configure the router as a BGP route reflector and configure the specified neighbor as its client, use the **neighbor route-reflector-client** command in address family or router configuration mode. To indicate that the neighbor is not a client, use the **no** form of this command. **neighbor** {*ip address*| *ipv6 address peer group name*} **route reflector client** **no neighbor** {*ip-address*| *ipv6-address*| *peer-group-name*} **route-reflector-client** Cisco IOS IP Routing: BGP Command Reference (November 21, 2012), at 486 By default, all internal BGP (iBGP) speakers in an autonomous system must be fully meshed, and neighbors do not readvertise iBGP learned routes to neighbors, thus preventing a routing information loop. When all the clients are disabled, the local router is no longer a route reflector. If you use route reflectors, all iBGP speakers need not be fully meshed. In the route reflector model, an Internal BGP peer is configured to be a *route reflector* responsible for passing iBGP learned routes to iBGP neighbors. This scheme eliminates the need for each router to talk to every other router. Use the **neighbor route-reflector-client** command to configure the local router as the route reflector and the specified neighbor as one of its clients. All the neighbors configured with this command will be members of the client group and the remaining iBGP peers will be members of the nonclient group for the local route reflector. The **bgp client-to-client reflection** command controls client-to-client reflection. Cisco IOS IP Routing: BGP Command Reference (November 21, 2012), at 487	**neighbor route-reflector-client** Participating BGP routers within an AS communicate EBGP-learned routes to all of their peers, but to prevent routing loops they must not re-advertise IBGP-learned routes within the AS. To ensure that all members of the AS share the same routing information, a fully meshed network topology (in which each member router of the AS is connected to every other member) can be used, but this topology can result in high volumes of IBGP messages when it is scaled. Instead, in larger networks one or more routers can be configured as route reflectors. A route reflector is configured to re-advertise routes learned through IBGP to a group of BGP neighbors within the AS (its clients), eliminating the need for a fully meshed topology. The **neighbor route-reflector-client** command configures the switch to act as a route reflector and configures the specified neighbor as one of its clients. Additional clients can be specified by re-issuing the command. The **bgp client-to-client reflection** command controls client-to-client reflection. The **no neighbor route-reflector-client** and **default neighbor route-reflector-client** commands disable route refection by deleting the **neighbor route-reflector-client** command from *running-config*. **Platform** all **Command Mode** Router-BGP Configuration **Command Syntax** **neighbor** *NEIGHBOR_ID* **route-reflector-client** **no neighbor** *NEIGHBOR_ID* **route-reflector-client** **default neighbor** *NEIGHBOR_ID* **route-reflector-client** Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1614
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 **neighbor ebgp-multihop** — Accepts and attempts BGP connections to external peers residing on networks that are not directly connected. Cisco IOS IP Routing: BGP Command Reference (November 21, 2012), at 416	**neighbor ebgp-multihop** The **neighbor ebgp-multihop** command programs the switch to accept and attempt BGP connections to the external peers residing on networks not directly connected to the switch. The command does not establish the multihop if the only route to the peer is the default route (0.0.0.0). Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1597

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 Cisco IOS IP Routing: BGP Command Reference (November 21, 2012), at 524	**neighbor route-map (BGP)** The neighbor route-map command applies a route map to inbound or outbound BGP routes. When a route map is applied to outbound routes, the switch will advertise only routes matching at least one section of the route map. Only one outbound route map and one inbound route map can be applied to a given neighbor. A new route map applied to a neighbor will replace the previous route map. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1613

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**show ip bgp ipv4 multicast summary** To display a summary of IP Version 4 multicast database-related information, use the **show ip bgp ipv4 multicast summary** command in EXEC mode. **show ip bgp ipv4 multicast summary** Cisco IOS IP Routing: BGP Command Reference (November 21, 2012), at 757 *Table 54: show ip bgp ipv4 multicast summary Field Descriptions* **Field** / **Description** Neighbor — IP address of configured neighbor in the multicast routing table. V — Version of multiprotocol BGP used. AS — Autonomous system to which the neighbor belongs. MsgRcvd — Number of messages received from the neighbor. MsgSent — Number of messages sent to the neighbor. TblVer — Number of the table version, which is incremented each time the table changes. InQ — Number of messages received in the input queue. OutQ — Number of messages ready to go in the output queue. Up/Down — Days and hours that the neighbor has been up or down (no information in the State column means the connection is up). State/PfxRcd — State of the neighbor/number of routes received. If no state is indicated, the state is up. Cisco IOS IP Routing: BGP Command Reference (November 21, 2012), at 758	**show ip bgp summary** The **show ip bgp summary** command displays BGP path, prefix, and attribute information for all BGP neighbors. Platform all Command Mode EXEC Command Syntax `show ip bgp summary [VRF_INSTANCE]` Parameters • *VRF_INSTANCE* specifies VRF instances. — <no parameter> displays routing table for context-active VRF. — **vrf** *vrf_name* displays routing table for the specified VRF. — **vrf all** displays routing table for all VRFs. — **vrf default** displays routing table for default VRF. Display Values **Header Row** • **BGP router identifier:** The router identifier – loopback address or highest IP address. • **Local AS Number:** AS number assigned to switch **Neighbor Table Columns** • (First) **Neighbor:** IP address of the neighbor. • (Second) **V:** BGP version number spoken to the neighbor • (Third) **AS:** Neighbor's Autonomous system number. • (Fourth) **MsgRcvd:** Number of messages received from the neighbor. • (Fifth) **MsgSent:** Number of messages sent to the neighbor. • (Sixth) **InQ:** Number of messages queued to be processed from the neighbor. • (Seventh) **OutQ:** Number of messages queued to be sent to the neighbor. • (Eighth) **Up/Down:** Period the BGP session has been in Established state or its current status. • (Ninth) **State:** State of the BGP session and the number of routes received from a neighbor. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1641

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco IOS 15.4

Effective date of registration: 11/26/2014</td>
<td>The following is sample output from the show ip bgp paths command in privileged EXEC mode:

<pre>Router# show ip bgp paths

Address   Hash Refcount Metric Path
0x60E5742C   0   1   0 i
0x60E3D7AC   2   1   0 ?
0x60E5C6C0   11   3   0 10 ?
0x60E577B0   35   2   40 10 ?</pre>
The table below describes the significant fields shown in the display.

Table 64: show ip bgp paths Field Descriptions
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Address</td><td>Internal address where the path is stored.</td></tr>
<tr><td>Hash</td><td>Hash bucket where path is stored.</td></tr>
<tr><td>Refcount</td><td>Number of routes using that path.</td></tr>
<tr><td>Metric</td><td>The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)</td></tr>
<tr><td>Path</td><td>The autonomous system path for that route, followed by the origin code for that route.</td></tr>
</table>

Cisco IOS IP Routing: BGP Command Reference (November 21, 2012), at 795</td>
<td>show ip bgp paths

The show ip bgp paths command displays all BGP paths in the database.

Platform all
Command Mode EXEC

Command Syntax
show ip bgp paths [VRF_INSTANCE]

Parameters
• VRF_INSTANCE specifies VRF instances.
— <no parameter> displays routing table for context-active VRF.
— vrf vrf_name displays routing table for the specified VRF.
— vrf all displays routing table for all VRFs.
— vrf default displays routing table for default VRF.

Display Values
• Refcount: Number of routes using a listed path.
• Metric: The Multi Exit Discriminator (MED) metric for the path.
• Path: The autonomous system path for that route, followed by the origin code for that route.

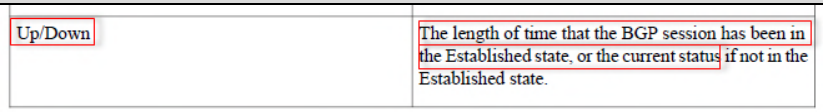
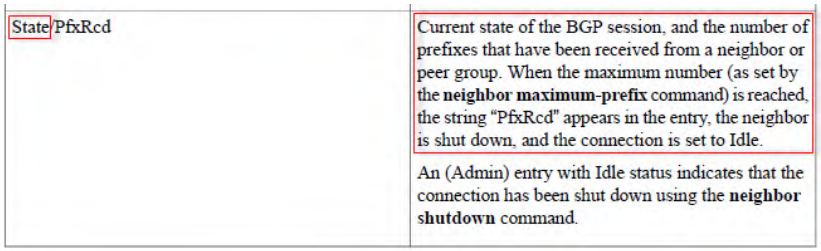
Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1638</td>
</tr>
<tr>
<td>Cisco IOS 15.4

Effective date of registration: 11/26/2014</td>
<td>The show ip bgp summary command is used to display BGP path, prefix, and attribute information for all connections to BGP neighbors.

Cisco IOS IP Routing: BGP Command Reference (November 21, 2012), at 819</td>
<td>show ip bgp summary

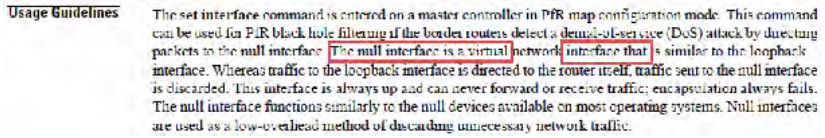
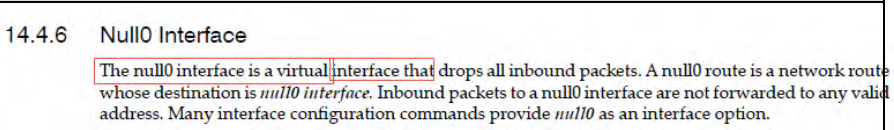
The show ip bgp summary command displays BGP path, prefix, and attribute information for all BGP neighbors.

Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1641</td>
</tr>
</table>

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 Up/Down — The length of time that the BGP session has been in the Established state, or the current status if not in the Established state. Cisco IOS IP Routing: BGP Command Reference (November 21, 2012), at 821  State/PfxRcd — Current state of the BGP session, and the number of prefixes that have been received from a neighbor or peer group. When the maximum number (as set by the **neighbor maximum-prefix** command) is reached, the string "PfxRcd" appears in the entry, the neighbor is shut down, and the connection is set to Idle. An (Admin) entry with Idle status indicates that the connection has been shut down using the **neighbor shutdown** command. Cisco IOS IP Routing: BGP Command Reference (November 21, 2012), at 822	**Neighbor Table Columns** • **(First) Neighbor:** IP address of the neighbor. • **(Second) V:** BGP version number spoken to the neighbor • **(Third) AS:** Neighbor's Autonomous system number. • **(Fourth) MsgRcvd:** Number of messages received from the neighbor. • **(Fifth) MsgSent:** Number of messages sent to the neighbor. • **(Sixth) InQ:** Number of messages queued to be processed from the neighbor. • **(Seventh) OutQ:** Number of messages queued to be sent to the neighbor. • **(Eighth) Up/Down:** Period the BGP session has been in Established state or its current status. • **(Ninth) State:**State of the BGP session and the number of routes received from a neighbor. After the maximum number of routes are received (maximum paths (BGP)), the field displays PfxRcd, the neighbor is shut down, and the connection is set to Idle. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1641

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**bfd** To set the baseline Bidirectional Forwarding Detection (BFD) session parameters on an interface, use the **bfd** command in interface configuration mode. To remove the baseline BFD session parameters, use the **no** form of this command. **bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value* **no bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier value* **Syntax Description** **interval** *milliseconds* — Specifies the rate, in milliseconds, at which BFD control packets will be sent to BFD peers. The valid range for the *milliseconds* argument is from 50 to 999. **min_rx** *milliseconds* — Specifies the rate, in milliseconds, at which BFD control packets will be expected to be received from BFD peers. The valid range for the *milliseconds* argument is from 50 to 999. **multiplier** *multiplier-value* — Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD declares that the peer is unavailable and the Layer 3 BFD peer is informed of the failure. The valid range for the *multiplier value* argument is from 3 to 50. Cisco IOS IP Routing: Protocol-Independent Command Reference (2013), at 9	**bfd** The **bfd** command configures BFD parameters for the configuration mode interface. All BFD sessions that pass through this interface will use these parameters. If custom parameters are not configured, the interface will use default values for BFD sessions passing through it. For a BFD session to be established, BFD must be enabled for any routing protocol using BFD for failure detection. The **no bfd** and **default bfd** commands return the BFD parameters on the configuration mode interface to default values by removing the corresponding **bfd** command from *running-config*. **Platform** all **Command Mode** Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Management Configuration Interface-Port-channel Configuration Interface-VLAN Configuration **Command Syntax** **bfd interval** *transmit_rate* **min_rx** *receive_minimum* **multiplier** *factor* **no bfd** **default bfd** **Parameters** • *transmit_rate* specifies the rate in milliseconds at which BFD control packets will be sent to BFD peers. Values range from 50 to 60000; the default value is 300. • *receive_minimum* specifies the rate in milliseconds at which BFD control packets will be expected from BFD peers. Values range from 50 to 60000. • *factor* specifies the number of consecutive missed BFD control packets from a BFD peer that will designate the peer as unavailable and indicate failure to the Layer 3 BFD peer. Values range from 3 to 50. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1741

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**ip route** To establish static routes, use the **ip route** command in global configuration mode. To remove static routes, use the **no** form of this command. **ip route** [**vrf** *vrf name*] *prefix mask* {*ip address*| *interface type interface number* [*ip address*]} [**dhcp**] [**global**] [*distance*] [**multicast**] [**name** *next-hop-name*] [**permanent**| **track** *number*] [**tag** *tag*] **no ip route** [**vrf** *vrf name*] *prefix mask* {*ip address*| *interface type interface number* [*ip address*]} [**dhcp**] [**global**] [*distance*] **multicast** [**name** *next-hop-name*] [**permanent**| **track** *number*] [**tag** *tag*] Cisco IOS IP Routing: Protocol-Independent Command Reference (2013), at 62 If you specify an administrative distance, you are flagging a static route that can be overridden by dynamic information. For example, routes derived with Enhanced Interior Gateway Routing Protocol (EIGRP) have a default administrative distance of 100. To have a static route that would be overridden by an EIGRP dynamic route, specify an administrative distance greater than 100. Static routes have a default administrative distance of 1. Cisco IOS IP Routing: Protocol-Independent Command Reference (2013), at 63	**ip route** The **ip route** command creates a static route. The destination is a network segment; the nexthop address is either an IPv4 address or a routable port. When multiple routes exist to a destination prefix, the route with the lowest administrative distance takes precedence. Static routes have a default administrative distance of 1. Assigning a higher administrative distance to a static route configures it to be overridden by dynamic routing data. For example, a static route with a distance value of 200 is overridden by OSPF intra-area routes with a default distance of 110. . . . Command Syntax **ip route** [*VRF_INSTANCE*] *dest_net* ***NEXTHOP*** [*DISTANCE*] [*TAG_OPTION*] [*RT_NAME*] **no ip route** [*VRF_INSTANCE*] *dest_net* [*NEXTHOP*] [*DISTANCE*] **default ip route** [*VRF_INSTANCE*] *dest_net* [*NEXTHOP*] [*DISTANCE*] Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1287
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**show ipv6 route summary** — Displays the current contents of the IPv6 routing table in summary format. Cisco IOS IP Routing: Protocol-Independent Command Reference (2013), at 284	**show ipv6 route summary** The **show ipv6 route summary** command displays the current contents of the IPv6 routing table in summary format. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1337
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**Usage Guidelines** Learn lists are a way to categorize learned traffic classes. In each learn list, different criteria for learning traffic classes including prefixes, application definitions, filters, and aggregation parameters can be configured. A traffic class is automatically learned by PfR based on each learn list criteria, and each learn list is configured with a sequence number. The sequence number determines the order in which learn list criteria are applied. Learn lists allow different PfR policies to be applied to each learn list; in previous releases the traffic classes could not be divided, and a PfR policy was applied to all the traffic classes profiled during one learning session. Cisco IOS Performance Routing Command Reference (2010), at 131	Route maps define conditions for redistributing routes between routing protocols. A route map clause is identified by a name, filter type (permit or deny) and sequence number. Clauses with the same name are components of a single route map; the sequence number determines the order in which the clauses are compared to a route. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 894

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 **Usage Guidelines** The set interface command is entered on a master controller in PfR map configuration mode. This command can be used for PfR black hole filtering if the border routers detect a denial-of-service (DoS) attack by directing packets to the null interface. The null interface is a virtual network interface that is similar to the loopback interface. Whereas traffic to the loopback interface is directed to the router itself, traffic sent to the null interface is discarded. This interface is always up and can never forward or receive traffic; encapsulation always fails. The null interface functions similarly to the null devices available on most operating systems. Null interfaces are used as a low-overhead method of discarding unnecessary network traffic. Cisco IOS Performance Routing Command Reference (2010), at 226	 14.4.6 Null0 Interface The null0 interface is a virtual interface that drops all inbound packets. A null0 route is a network route whose destination is *null0 interface*. Inbound packets to a null0 interface are not forwarded to any valid address. Many interface configuration commands provide *null0* as an interface option. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 633

Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	snmp-server enable traps pfr
	
	To enable Performance Routing (PfR) Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **snmp server enable traps pfr** command in global configuration mode. To disable PfR notifications, use the no form of this command.
	
	snmp-server enable traps pfr
	no snmp-server enable traps pfr
	
	Syntax Description This command has no arguments or keywords.
	
	Command Default PfR SNMP notifications are disabled.
	
	Command Modes Global configuration (config)
	
	Command History
	Release — **Modification**
	Cisco IOS XE Release 3.7S — This command was introduced.
	15.3(2)T — This command was integrated into Cisco IOS Release 15.3(2)T
	
	Usage Guidelines Use this command to enable SNMP notifications for PfR activity.
	
	Examples This example shows how to enable PfR SNMP notifications:
	
	`Router(config)# snmp server host 10.2.2.2 traps public ptr`
	`Router(config)# snmp-server enable traps pfr`
	`Router(config)# exit`
	
	Cisco IOS Performance Routing Command Reference (2010), at 372
		snmp-server enable traps
		
		The **snmp-server enable traps** command enables the transmission of Simple Network Management Protocol (SNMP) notifications as traps or inform requests. This command enables both traps and inform requests for the specified notification types. The **snmp-server host** command specifies the notification type (traps or informs). Sending notifications requires at least one **snmp-server host** command.
		
		The **snmp-server enable traps** and **no snmp-server enable traps** commands, without an MIB parameter, specifies the default notification trap generation setting for all MIBs. These commands, when specifying an MIB, controls notification generation for the specified MIB. The **default snmp-server enable traps** command resets notification generation to the default setting for the specified MIB.
		
		Platform — all
		Command Mode — Global Configuration
		
		Command Syntax
		`snmp-server enable traps [trap_type]`
		`no snmp-server enable traps [trap_type]`
		`default snmp-server enable traps [trap_type]`
		
		Parameters
		• *trap_type* controls the generation of informs or traps for the specified MIB:
		— <no parameter> controls notifications for MIBs not covered by specific commands.
		— **entity** controls entity-MIB modification notifications.
		— **lldp** controls LLDP notifications.
		— **msdpBackwardTransition** controls msdpBackwardTransition notifications.
		— **msdpEstablished** controls msdpEstablished notifications.
		— **snmp** controls SNMP-v2 notifications.
		— **switchover** controls switchover notifications.
		— **snmpConfigManEvent** controls snmpConfigManEvent notifications.
		— **test** controls test traps.
		
		Examples
		• These commands enables notification generation for all MIBs except spanning tree.
		`switch(config)#snmp-server enable traps`
		`switch(config)#no snmp-server enable traps spanning-tree`
		`switch(config)#`
		• This command enables spanning-tree MIB notification generation, regardless of the default setting.
		`switch(config)#snmp-server enable traps spanning-tree`
		`switch(config)#`
		
		Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1990

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**no snmp-server** To disable Simple Network Management Protocol (SNMP) agent operation, use the **no snmp** server command in global configuration mode. `no snmp server` **Syntax Description** This command has no arguments or keywords. **Command Default** No default behavior or values. **Command Modes** Global configuration **Command History** | Release	Modification
---	---

10.0	This command was introduced. |
	
	Usage Guidelines This command disables all running versions of SNMP (SNMPv1, SNMPv2C, and SNMPv3) on the device.
	
	Examples The following example disables the current running version of SNMP:
	
	`Router(config)# no snmp-server`
	
	Cisco IOS SNMP Support Command Reference (2013), at 52
		no snmp-server
		
		The no snmp-server and default snmp-server commands disable Simple Network Management Protocol (SNMP) agent operation by removing all snmp-server commands from *running-config*.
		
		SNMP is enabled with any snmp-server community or snmp-server user command.
		
		Platform all
		Command Mode Global Configuration
		
		Command Syntax
		
		`no snmp-server`
		`default snmp-server`
		
		Example
		
		• This command disables SNMP agent operation on the switch
		
		`switch(config)#no snmp-server`
		`switch(config)#`
		
		Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1973

Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	Examples The following is sample output from the **show snmp** command:
	
	`Router# show snmp`
	`Chassis: 12161083`
	`0 SNMP packets input`
	`0 Bad SNMP version errors`
	`0 Unknown community name`
	`0 Illegal operation for community name supplied`
	`0 Encoding errors`
	`0 Number of requested variables`
	`0 Number of altered variables`
	`0 Get-request PDUs`
	`0 Get-next PDUs`
	`0 Set-request PDUs`
	`0 Input queue packet drops (Maximum queue size 1000)`
	`0 SNMP packets output`
	`0 Too big errors (Maximum packet size 1500)`
	`0 No such name errors`
	`0 Bad values errors`
	`0 General errors`
	`0 Response PDUs`
	`0 Trap PDUs`
	`SNMP logging: enabled`
	`SNMP Trap Queue: 0 dropped due to resource failure.`
	
	Cisco IOS SNMP Support Command Reference (2013), at 83
		Example
		• This command configures *xyz-1234* as the chassis-ID string, then displays the result.
		
		`switch(config)#snmp-server chassis-id xyz-1234`
		`switch(config)#show snmp`
		`Chassis: xyz-1234` *<---chassis ID*
		
		`8 SNMP packets input`
		`0 Bad SNMP version errors`
		`0 Unknown community name`
		`0 Illegal operation for community name supplied`
		`0 Encoding errors`
		`8 Number of requested variables`
		`0 Number of altered variables`
		`4 Get-request PDUs`
		`4 Get-next PDUs`
		`0 Set-request PDUs`
		`21 SNMP packets output`
		`0 Too big errors`
		`0 No such name errors`
		`0 Bad value errors`
		`0 General errors`
		`8 Response PDUs`
		`0 Trap PDUs`
		`SNMP logging: enabled`
		`Logging to taccon.162`
		`SNMP agent enabled`
		`switch(config)#`
		
		Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1967-68

Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	show snmp engineID
	
	To display the identification of the local Simple Network Management Protocol (SNMP) engine and all remote engines that have been configured on the router, use the show **snmp engineID** command in EXEC mode.
	
	show **snmp engineID**
	
	Syntax Description This command has no arguments or keywords.
	
	Command Modes EXEC
	
	Command History
	
	Release / **Modification**
	12.0(3)T / This command was introduced
	12.2(33)SRA / This command was integrated into Cisco IOS Release 12.2(33)SRA
	12.2SX / This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
	
	Usage Guidelines An SNMP engine is a copy of SNMP that can reside on a local or remote device.
	
	Examples The following example specifies 0000000902000000C025808 as the local engineID and 123456789ABCDEF000000000 as the remote engine ID, 172.16.37.61 as the IP address of the remote engine (copy of SNMP) and 162 as the port from which the remote device is connected to the local device:
	
	Router# show snmp engineID
	Local SNMP engineID: 0000000902000000C025808
	Remote Engine ID IP-addr Port
	123456789ABCDEF000000000 172.16.37.61 162
	The table below describes the fields shown in the display.
	
	Cisco IOS SNMP Support Command Reference (2013), at 91
		show snmp engineID
		
		The show snmp engineID command displays the identification of the local Simple Network Management Protocol (SNMP) engine and of all remote engines that are configured on the switch.
		
		Platform all
		Command Mode EXEC
		
		Command Syntax
		`show snmp engineID`
		
		Example
		• This command displays the ID of the local SNMP engine.
		
		`switch>show snmp engineid`
		`Local SNMP EngineID: f5717f001c730436d700`
		`switch>`
		
		Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1978

Cisco IOS 15.4 Effective date of registration: 11/26/2014	**Related Commands** **Command** / **Description** snmp server **engineID local** / Configures a name for either the local or remote SNMP engine on the router. Cisco IOS SNMP Support Command Reference (2013), at 92	**Configuring the Engine ID** The snmp-server engineID remote command configures the name for the local or remote Simple Network Management Protocol (SNMP) engine. An SNMP engine ID is a name for the local or remote SNMP engine. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1966

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	security model — The security model used by the group, either v1, v2c, or v3. Cisco IOS SNMP Support Command Reference (2013), at 92	• *VERSION* the security model used by the group. — **v1** SNMPv1. Uses a community string match for authentication. — **v2c** SNMPv2c. Uses a community string match for authentication. — **v3 no auth** SNMPv3. Uses a username match for authentication. — **v3 auth** SNMPv3. HMAC-MD5 or HMAC-SHA authentication. — **v3 priv** SNMPv3. HMAC-MD5 or HMAC-SHA authentication. AES or DES encryption. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1994

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**show snmp host** To display the recipient details for Simple Network Management Protocol (SNMP) notification operations, use the show snmp host command in privileged EXEC mode. show snmp host **Syntax Description** This command has no arguments or keywords. **Command Default** The information configured for SNMP notification operation is displayed. **Command Modes** Privileged EXEC (#) **Command History** Release: 12.4(12)T — Modification: This command was introduced 12.2(31)SB — This command was integrated into Cisco IOS Release 12.2(31)SB2. 12.2SX — This command was integrated into Cisco IOS Release 12.2SX. **Usage Guidelines** The show snmp host command displays details such as IP address of the Network Management System (NMS), notification type, SNMP version, and the port number of the NMS. To configure these details, use the snmp-server host command. **Examples** The following is sample output from the show snmp host command. Router# show snmp host Notification host: 10.2.28.6 udp-port: 162 type: inform user: public security model: v2c traps: ... The table below describes the significant fields shown in the display. *Table 5: show snmp host Field Descriptions* Field: Notification host — Description: Displays the IP address of the host for which the notification is generated. udp-port — Displays the port number. type — Displays the type of notification. Field: user — Description: Displays the access type of the user for which the notification is generated. security model — Displays the SNMP version used to send notifications. traps — Displays details of the notification generated. **Related Commands** Command: snmp-server host — Description: Configures the recipient details for SNMP notification operations. Cisco IOS SNMP Support Command Reference (2013), at 95-96	**show snmp host** The show snmp host command displays the recipient details for Simple Network Management Protocol (SNMP) notification operations. Details that the command displays include IP address and port number of the Network Management System (NMS), notification type, and SNMP version. Platform: all Command Mode: EXEC Command Syntax show snmp host Field Descriptions • Notification host — IP address of the host for which the notification is generated. • udp-port — port number. • type — notification type. • user — access type of the user for which the notification is generated. • security model — SNMP version used to send notifications. • traps — details of the notification generated. Example • This command displays the hosts configured on the switch. switch>show snmp host Notification host: 172.22.22.20 udp-port: 162 type: trap user: public security model: v2c switch> Arista User Manual v.4.14.3F (Rev. 2) (October 2, 2014), at 1980

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**show snmp location** To display the Simple Network Management Protocol (SNMP) system location string, use the show snmp locationcommand in privileged EXEC mode. **show snmp location** **Syntax Description** This command has no arguments or keywords. **Command Default** The SNMP system location information is displayed. **Command Modes** Privileged EXEC (#) **Command History** Release: 12.4(12)T — Modification: This command was introduced 12.2(31)SB — This command was integrated into Cisco IOS Release 12.2(31)SB2 12.2SX — This command was integrated into Cisco IOS Release 12.2SX. **Usage Guidelines** To configure system location details, use the snmp-server locationcommand. Cisco IOS SNMP Support Command Reference (2013), at 97	**show snmp location** The show snmp location command displays the Simple Network Management Protocol (SNMP) system location string. The snmp-server location command configures system location details. The command has no effect if a location string was not previously configured. Platform all Command Mode EXEC Command Syntax `show snmp location` Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1980
Cisco IOS 15.4 Effective date of registration: 11/26/2014	SNMP management information is viewed as a collection of managed objects, residing in a virtual information store, termed the Management Information Base (MIB). Collections of related objects are defined in MIB modules. These modules are written using a subset of OSIs Abstract Syntax Notation One (ASN.1), termed the Structure of Management Information (SMI). Cisco IOS SNMP Support Command Reference (2013), at 98	• **Management Information Base (MIB):** The MIB stores network management information, which consists of collections of managed objects. Within the MIB are collections of related objects, defined in MIB modules. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1961
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**show snmp group** — Displays the names of configured SNMP groups, the security model being used, the status of the different views, and the storage type of each group. Cisco IOS SNMP Support Command Reference (2013), at 123	**show snmp group** The show snmp group command displays the names of configured SNMP groups along with the security model, and view status of each group. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1971

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**show snmp view** — Displays the family name, storage type, and status of an SNMP configuration and associated MIB. Cisco IOS SNMP Support Command Reference (2013), at 123	**show snmp view** The show snmp view command displays the family name, storage type, and status of a Simple Network Management Protocol (SNMP) configuration and the associated MIB. SNMP views are configured with the snmp-server view command. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1986

Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	snmp-server group — Configures a new SNMP group or a table that maps SNMP users to SNMP views.
	snmp-server trap authentication vrf — Controls VRF-specific SNMP authentication failure notifications.
	snmp-server user — Configures a new user to an SNMP group.
	
	Cisco IOS SNMP Support Command Reference (2013), at 130
		Configuring the Group
		
		An SNMP group is a table that maps SNMP users to SNMP views. The snmp-server group command configures a new SNMP group.
		
		Example
		• This command configures *normal_one* as an SNMPv3 group (authentication and encryption) that provides access to the *all-items* read view.
		`switch(config)#snmp-server group normal_one v3 priv read all-items`
		`switch(config)#`
		
		Configuring the User
		
		An SNMP user is a member of an SNMP group. The snmp-server user command adds a new user to an SNMP group and configures that user's parameters. To configure a remote user, specify the IP address or port number of the device where the user's remote SNMP agent resides.
		
		Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1966

Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	snmp trap link-status
	
	To enable Simple Network Management Protocol (SNMP) link trap generation, use the **snmp trap link-status** command in either interface configuration mode or service instance configuration mode. To disable SNMP link trap generation, use the **no** form of this command.
	
	snmp trap link-status [**permit duplicates**]
	no snmp trap link-status [**permit duplicates**]
	
	Cisco IOS SNMP Support Command Reference (2013), at 130
		snmp trap link-status
		
		The **snmp trap link-status** command enables Simple Network Management Protocol (SNMP) link-status trap generation on the configuration mode interface. The generation of link-status traps is enabled by default. If SNMP link-trap generation was previously disabled, this command removes the corresponding **no snmp link-status** statement from the configuration to re-enable link-trap generation.
		
		The **no snmp trap link-status** command disables SNMP link trap generation on the configuration mode interface.
		
		The **snmp trap link-status** and **default snmp trap link-status** commands restore the default behavior by removing the **no snmp trap link-status** command from *running-config*. Only the no form of this command is visible in *running-config*.
		
		Platform: all
		Command Mode: Interface-Ethernet Configuration
		Interface-Loopback Configuration
		Interface-Management Configuration
		Interface-Port-channel Configuration
		Interface-VLAN Configuration
		Interface-VXLAN Configuration
		
		Command Syntax
		`snmp trap link-status`
		`no snmp trap link-status`
		`default snmp trap link-status`
		
		Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1966

Cisco IOS 15.4 Effective date of registration: 11/26/2014	**snmp-server host** — Specifies the targeted recipient of an SNMP notification operation. Cisco IOS SNMP Support Command Reference (2013), at 191	**Configuring the Host** The **snmp-server host** command specifies the recipient of a SNMP notification. An SNMP host is the recipient of an SNMP trap operation. The **snmp-server host** command sets the community string if it was not previously configured. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1967
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**Usage Guidelines** SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests. Cisco IOS SNMP Support Command Reference (2013), at 216	The **snmp-server enable traps** command enables the transmission of Simple Network Management Protocol (SNMP) notifications as traps or inform requests. This command enables both traps and inform requests for the specified notification types. The **snmp-server host** command specifies the notification type (traps or informs). Sending notifications requires at least one **snmp-server host** command. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1990

Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	snmp-server engineID local
	
	To specify the Simple Network Management Protocol (SNMP) engine ID on the local device, use the snmp-server engineID local command in global configuration mode. To remove the configured engine ID, use the no form of this command.
	
	snmp-server engineID local *engine-id-string*
	no snmp-server engineID local *engine-id-string*
	
	Syntax Description
	engine-id-string — String of a maximum of 24 characters that identifies the engine ID.
	
	Command Default
	An SNMP engine ID is generated automatically but is not displayed or stored in the running configuration. You can display the default or configured engine ID by using the show snmp engineID command.
	
	Command Modes
	Global configuration (config)
	
	Command History
	Release — Modification
	12.0(3)T — This command was introduced.
	12.2(33)SRA — This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX — This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
	
	Usage Guidelines
	The SNMP engine ID is a unique string used to identify the device for administrative purposes. You do not need to specify an engine ID for the device, a default string is generated using Cisco's enterprise number (1.3.6.1.4.1.9) and the MAC address of the first interface on the device. For further details on the SNMP engine ID, see RFC 2571.
	If you specify your own ID, note that the entire 24-character engine ID is not needed if it contains trailing zeros. Specify only the portion of the engine ID up until the point where only zeros remain in the value. For example, to configure an engine ID of 123400000000000000000000, you can specify snmp-server engineID local 1234.
	The value for the engine ID is displayed in hexadecimal value pairs. If the length of the input is an odd number, the last digit will be prepended with a zero ("0"). For example, if the engine ID is 12345, the ID is treated as 123405 internally. Hence, the engine ID is displayed as 123405 in the show running-configuration command output.
	Changing the value of the SNMP engine ID has significant effects. A user's password (entered on the command line) is converted to a message digest algorithm (MD5) or Secure Hash Algorithm (SHA) security digest. This digest is based on both the password and the local engine ID. The command line password is then destroyed, as required by RFC 2274. Because of this deletion, if the local value of the engineID changes, the security digests of SNMPv3 users will become invalid, and the users will have to be reconfigured.
	Similar restrictions require the reconfiguration of community strings when the engine ID changes. A remote engine ID is required when an SNMPv3 inform is configured. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.
	
	Examples
	The following example specifies the local SNMP engine ID:
	Router(config)# snmp-server engineID local 1234
	
	Cisco IOS SNMP Support Command Reference (2013), at 339-340
		snmp-server engineID local
		
		The snmp-server engineID local command configures the name for the local Simple Network Management Protocol (SNMP) engine. The default SNMP engineID is generated by the switch and is used when an engineID is not configured with this command. The show snmp engineID command displays the default or configured engine ID.
		
		SNMPv3 authenticates users through security digests (MD5 or SHA) that are based on user passwords and the local engine ID. Passwords entered on the CLI are similarly converted, then compared to the user's security digest to authenticate the user.
		
		Important Changing the local engineID value invalidates SNMPv3 security digests, requiring the reconfiguration of all user passwords.
		
		The no snmp-server engineID and default snmp-server engineID commands restore the default engineID by removing the snmp-server engineID command from the configuration.
		
		Platform — all
		Command Mode — Global Configuration
		
		Command Syntax
		`snmp-server engineID local engine_hex`
		`no snmp-server engineID local`
		`default snmp-server engineID`
		
		Parameters
		• *engine_hex* the switch's name for the local SNMP engine (hex string).
		The string must consist of at least ten characters with a maximum of 64 characters.
		
		Example
		• This command configures DC945798CAB4 as the name of the local SNMP engine.
		`switch(config)#snmp-server engineID local DC945798CAB4`
		`switch(config)#`
		
		snmp-server engineID remote
		
		The snmp-server engineID remote command configures the name of a Simple Network Management Protocol (SNMP) engine located on a remote device. The switch generates a default engineID; use the show snmp engineID command to view the configured or default engineID.
		
		A remote engine ID is required when configuring an SNMPv3 inform to compute the security digest for authenticating and encrypting packets sent to users on the remote host. SNMPv3 authenticates users through security digests (MD5 or SHA) that are based on user passwords and the engine ID. Passwords entered on the CLI are similarly converted, then compared to the user's security digest to authenticate the user.
		
		Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1991-92

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show snmp engineID</td><td>Displays the identification of the local SNMP engine and all remote engines that have been configured on the router.</td></tr></table> Cisco IOS SNMP Support Command Reference (2013), at 340	**show snmp engineID** The show snmp engineID command displays the identification of the local Simple Network Management Protocol (SNMP) engine and of all remote engines that are configured on the switch. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1978

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	**snmp-server group** To configure a new Simple Network Management Protocol (SNMP) group, use the **snmp server group** command in global configuration mode. To remove a specified SNMP group, use the **no** form of this command. **snmp server group** *group name* {**v1**| **v2c**| **v3** {**auth**| **noauth**| **priv**}} [**context** *context name*] [**read** *read view*] [**write** *write-view*] [**notify** *notify-view*] [**access** [**ipv6** *named-access-list*] [*acl-number*| *acl-name*]] **no snmp-server group** *group-name* {**v1**| **v2c**| **v3** {**auth**| **noauth**| **priv**}} [**context** *context-name*] **Syntax Description** *group-name* — Name of the group. **v1** — Specifies that the group is using the SNMPv1 security model. SNMPv1 is the least secure of the possible SNMP security models. **v2c** — Specifies that the group is using the SNMPv2c security model. The SNMPv2c security model allows informs to be transmitted and supports 64-character strings. **v3** — Specifies that the group is using the SNMPv3 security model. SNMPv3 is the most secure of the supported security models. It allows you to explicitly configure authentication characteristics. **auth** — Specifies authentication of a packet without encrypting it. **noauth** — Specifies no authentication of a packet. **priv** — Specifies authentication of a packet with encryption. **context** — (Optional) Specifies the SNMP context to associate with this SNMP group and its views. *context name* — (Optional) Context name. **read** — (Optional) Specifies a read view for the SNMP group. This view enables you to view only the contents of the agent.	**snmp-server group** The snmp-server group command configures a new Simple Network Management Protocol (SNMP) group or modifies an existing group. An SNMP group is a data structure that user statements reference to map SNMP users to SNMP contexts and views, providing a common access policy to the specified users. An SNMP context is a collection of management information items accessible by an SNMP entity. Each item of may exist in multiple contexts. Each SNMP entity can access multiple contexts. A context is identified by the EngineID of the hosting device and a context name. The no snmp-server group and default snmp-server group commands delete the specified group by removing the corresponding snmp-server group command from the configuration. Platform all Command Mode Global Configuration Command Syntax **snmp-server group** *group_name* ***VERSION*** [***CNTX***] [***READ***] [***WRITE***] [***NOTIFY***] **no snmp-server group** *group_name* ***VERSION*** **default snmp-server group** *group_name* ***VERSION*** Parameters • *group_name* the name of the group. • *VERSION* the security model used by the group. — v1 SNMPv1. Uses a community string match for authentication. — v2c SNMPv2c. Uses a community string match for authentication. — v3 no auth SNMPv3. Uses a username match for authentication. — v3 auth SNMPv3. HMAC-MD5 or HMAC-SHA authentication. — v3 priv SNMPv3. HMAC-MD5 or HMAC-SHA authentication. AES or DES encryption. • *CNTX* associates the SNMP group to an SNMP context. — <no parameter> command does not associate group with an SNMP context. — context *context_name* associates group with context specified by *context_name*. • *READ* specifies read view for SNMP group. — <no parameter> command does not specify read view. — read *read_name* read view specified by *read_name* (string – maximum 64 characters). • *WRITE* specifies write view for SNMP group. — <no parameter> command does not specify write view. — write *write_name* write view specified by *write_name* (string – maximum 64 characters). • *NOTIFY* specifies notify view for SNMP group. — <no parameter> command does not specify notify view. — notify *notify_name* notify view specified by *notify_name* (string – maximum 64 characters).